Ashley M. Gjovik, JD
In Propria Persona
2108 N St. Ste. 4553
Sacramento, CA, 95816
(408) 883-4428
legal@ashleygjovik.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ASHLEY M. GJOVIK,
an individual,

Plaintiff,

vs.

APPLE INC.,
a corporation,

Defendant.

CASE NO.
3:23-CV-04597-EMC (KAW)

PLAINTIFF'S DECLARATION IN SUPPORT OF: PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION AT DKT. 294

HEARING:
Location: Oakland (TBD)
Date: April 2 2026
Time: 1:30 PM

PLAINTIFF'S DECLARATION (DKT. 294)
DECLARATION OF ASHLEY M. GJOVIK,
IN SUPPORT OF PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION AT DKT. 294, AND IN SUPPORT OF PLAINTIFF'S REQUEST FOR JUDICIAL NOTICE

Plaintiff Ashley Gjovik respectfully files this Declaration in support of her Opposition to Defendant Apple Inc.'s Motion to Enforce Protective Order (Dkt. 294) and in compliance with Civil L.R. 7-3, 7-4, and 7-5.

I, Ashley M. Gjovik, declare as follows:

1. I am the Plaintiff in the above-captioned matter, appearing In Propria Persona. I have personal knowledge of the facts stated herein and, if called as a witness, could and would testify competently thereto.
2. I make this Declaration in support of my Opposition to Defendant's Motion to Enforce Protective Order (Dkt. 294), my Motion for Judicial Notice, and my Motion for Sanctions under Fed. R. Civ. P. 26(g) (Dkt. 302).

EXHIBITS — PRESS AND MEDIA COVERAGE

3. Attached hereto as Exhibit A is a true and correct copy of the article titled ***"Apple Cares About Privacy Unless You Work at Apple***," published on or about August 30–31, 2021. This article quotes me describing what I felt were invasions of my privacy by Apple, including with its studies and its surveillance practices, with its collection of nude photos of me, and with workplace retaliation. The journalist contacted Apple for comment prior to publication. Apple did not respond. Apple terminated my employment approximately ten days after publication. Apple subsequently cited this article as the basis for my termination. *See* Dkt. 280 fn. 2.
4. Attached hereto as Exhibit B is a true and correct copy of the article titled "***Apple lädt Mitarbeiter zu Datenparty – um Gesichter zu scannen***,"published by Der Spiegel, on or about June 24 2022. The German original version is included followed by a version informally translated to English ("***iPhone is watching you***"). Der Spiegel is a publication of general circulation published in the Federal Republic of Germany. This article reports on Plaintiff's complaints about working conditions at Apple, Apple surveillance practices, and Apple's studies on employees. ("Gjovik now wants to reveal that the company is not only breaking its promises, but possibly also the law. … She is in contact with California's data protection authority about the violation of her privacy, and German authorities are also involved… For around four years, the app photographed her when

she was half asleep or on the toilet, and even nude pictures of her were stored. She estimates that the app took hundreds of pictures a day… She is now fighting her dismissal before the National Labor Relations Board (NLRB). According to SPIEGEL, the SEC is also interested in whether Apple wanted to shut down a whistleblower..") . I filed this article to the Ninth Circuit docket for case 25-2028 Dkt. 27-5 pp.27-31 on May 20 2025 and Apple was served with it. [Live URL: https://www.spiegel.de/netzwelt/gadgets/apple-laedt-mitarbeiter-zu-daten-party-um-gesichter-zu-scannen-a-54c4a2da-0f39-48be-9762-1bda39fcca8e].

5. Attached hereto as **Exhibit C** is a true and correct copy of the article titled ***"Ashley Gjøvik, lanceuse d'alerte licenciée par Apple, seule contre tous,"*** published by Telerama, a French publication, on or about March 14 2023. The French original version is included followed by a version informally translated to English ("***Ashley Gjevik, whistleblower fired by Apple, alone against all odds: The fault of this employee, who will be dismissed in 2021: she revealed that the Californian firm turns its employees into guinea pigs. Even stalking them in their private lives.")*** This article reports on Apple's studies on employees, complaints about invasions of privacy, and labor disputes at Apple. I filed this article to the Ninth Circuit docket for case 25-2028 Dkt. 27-5 pp.33-42 on May 20 2025 and Apple was served with it. [live URL: https://www.telerama.fr/debats-reportages/ashley-gjovik-lanceuse-d-alerte-licenciee-par-apple-seule-contre-tous-7014661.php].

6. Attached hereto as **Exhibit D** is a true and correct copy of the article titled "***Apple whistleblower brings spying claims to UK: Data watchdog opens investigation into privacy accusations against iPhone maker,"*** published by The Telegraph on or about April 10 2022. This article reports on Apple's employee "studies," complaints about invasion of privacy, and allegations of systemic regulatory noncompliance by Apple. I filed this article to the Ninth Circuit docket for case 25-2028 Dkt. 27-5 pp. 55-56 on May 20 2025 and Apple was served with it. ("Britain's information watchdog is investigating claims that Apple was able to access personal information on workers' phones after a privacy complaint was lodged by a whistleblower. Ashley Gjovik, a former senior Apple engineer, has filed a 54-page privacy complaint against the iPhone maker alleging unlawful data collection and invasion of employee privacy over "years and multiple countries" In the filing, which has been lodged with the UK Data Protection Information Commissioner's Office (ICO) and its counterpart in Brussels, Ms Gjovik claimed that she publicly expressed concerns about Apple "pressuring its employees to participate in invasive data collection procedures, including

scans of ears/ear canals".) [live URL: https://www.telegraph.co.uk/business/2022/04/10/apple-whistleblower-brings-spying-claims-uk/]

7. Attached hereto as **Exhibit E** is a true and correct copy of the article "***Ex-Apple employee takes Face ID privacy complaint to Europe,"*** published by TechCrunch and Yahoo! News around April 11 2022, and previously filed in to the Ninth Circuit case 25-2028 and Dkt. 27-5 at 63-64, and Apple was served. ("At the time, Gjøvik had been placed on administrative leave by Apple after raising concerns about sexism in the workplace, and a hostile and unsafe working environment which it had said it was investigating. She subsequently filed complaints against Apple with the U.S. National Labor Relations Board. Those earlier complaints link to the privacy complaint she's sent to international oversight bodies now because Gjøvik says she wants scrutiny of Apple's privacy practices after it formally told the U.S. government its reasons for firing her — and "felt comfortable admitting they'd fire employees for protesting invasions of privacy", as she puts it — accusing Apple of using her concerns over its approach to staff privacy as a pretext to terminate her for reporting wider safety concerns and organizing with other employees about labor concerns. The U.K.'s Information Commissioner's Offie (ICO) and France's CNIL both confirmed receipt of Gjøvik's privacy complaint against Apple. A spokesperson for the ICO told TechCrunch: "We are aware of this matter and we will assess the information provided." France's CNIL also sent confirmation that it's looking at Gjøvik's complaint.") (live URL: https://techcrunch.com/2022/04/11/gobbler-complaint-europe/)/
8. Attached hereto as **Exhibit F** is a true and correct copy of Gizmodo article: "***Apple Wanted Her Fired. It Settled on an Absurd Excuse The reasons for firing Ashley Gjøvik include tweeting a photo of herself—taken by her own phone,"*** ("Gjøvik deleted the tweets as asked, but retained counsel to respond to Apple. David L. Hecht, one of the nation's leading patent litigators, sent the company a letter on her behalf, dismantling Apple's claims bit by bit. "While I understand that Apple is not opposed to taking aggressive litigation postures (and indeed has a history of doing so)," Hecht wrote, "I remind you of your ethical duties as an attorney regarding the assertion of claims that have no basis in fact." Hecht noted, for instance, that the emails shared publicly by Gjøvik were neither labeled confidential nor contained anything "that could be considered secret or otherwise proprietary. "The posted image of the email merely noted what was already known to the public," he said. "It is no secret that Apple has been scanning a wide range of human ears… Hecht pointed to the fact that Apple's vice president of product marketing, Greg Joswiak, had

spoken publicly about scanning people's ears: "We had done work with Stanford to 3D-scan hundreds of different ears…"). Oct. 15 2021. [public URL: https://gizmodo.com/apple-wanted-her-fired-it-settled-on-an-absurd-excuse-1847868789]

9. Attached hereto as **Exhibit G** is a true and correct copy of Inverse article, "***Apple is leaning on weak arguments to defend a senior engineer's firing,"*** Oct. 15 2021, ("Now she's also working with the NLRB on a case alleging that Apple's anti-leaking policies actually violate U.S. law. Gjøvik alleges that an all-staff email from CEO Tim Cook stating that "people who leak confidential information do not belong here" violated the National Labor Relations Act, *Bloomberg* reports Gjøvik's latest filings claim that several other policies in the company's employee handbook — like restrictions on talking to reporters and revealing compensation — illegally interfere with workers' rights. Gjøvik's hope with all these legal proceedings is straightforward: to change what she sees as a poor working environment at Apple. "Ultimately," she told *Bloomberg*, "we're never going to see any systemic change at Apple without empowering the employees to feel comfortable speaking out as they are legally protected to.") [public URL: https://www.inverse.com/input/culture/apple-is-leaning-on-weak-arguments-to-defend-a-senior-engineers-firing]
10. Attached hereto as **Exhibit H** is a true and correct copy of Biometric Update article titled "***Ex-employee accuses Apple of training iPhone biometrics by violating staff privacy,"*** and published around April 20 2022. ("The company invited its employees to participate in product testing, and sometimes to have their biometrics collected, but Gjøvik says the testing and collection seemed to be mandatory. She describes the use of Apple's internal Gobbler app (later called Glimmer) to upload personal data employees had collected to company servers, and directly claims that employee data is the source of the billion images used to train Face ID.") (live URL: https://www.biometricupdate.com/202204/ex-employee-accuses-apple-of-training-iphone-biometrics-by-violating-staff-privacy).

EXHIBITS — APPLE'S OWN PUBLIC DISCLOSURES

11. Attached hereto as **Exhibit I** is a true and correct copy of the peer-reviewed article: Mahalingaiah, Shruthi et al. "**Design and methods of the Apple Women's Health Study: a digital longitudinal cohort study."** *American journal of obstetrics and gynecology* vol. 226,4 (2022): 545.e1-545.e29. doi:10.1016/j.ajog.2021.09.041, authored by Apple-affiliated researchers, Apple employees, and published in a peer-reviewed medical journal indexed in PubMed and other medical article

databases. This detailed, 24-page article describes the methodology of Apple's ovulation and menstruation studies ("*The Apple Women's Health Study was designed to gain a deeper understanding of the relationship among menstrual cycles, health, and behavior*."), and the paper covers topics including: "survey design," "Apple research app platform," "study population," "Eligibility, screening, and consent," "Recruitment and marketing," "Survey data," "Monthly surveys and timing," "Research sensor and usage data," "HealthKit data," "Principal findings," "Clinical implications," "Research implications," and "Strengths and limitations.". [live URL: https://pubmed.ncbi.nlm.nih.gov/34610322/]

12. Attached hereto as **Exhibit J** is a true and correct printout of the **ClinicalTrials.gov** registration for Apple's study, identifier NCT04196595, retrieved from https://clinicaltrials.gov. This is a public federal government database maintained by the National Institutes of Health. The "responsible party" is listed as Apple Inc and the study is "recruiting" participants. [live URL: https://clinicaltrials.gov/study/NCT04196595]
13. Attached hereto as **Exhibit K** is a true and correct printout of Apple's own website with a Sept. 10 2019 press release promoting "***three groundbreaking health studies***" including "***Apple Women's Health Study***: In partnership with Harvard T. H. Chan School of Public Health and the NIH's National Institute of Environmental Health Sciences (NIEHS), Apple has created the first long-term study of this scale focused on menstrual cycles and gynecological conditions." [live URL: https://www.apple.com/newsroom/2019/09/apple-announces-three-groundbreaking-health-studies/]

EXHIBITS — FEDERAL REGULATORY RECORDS

13. Attached hereto as **Exhibit L** is a true and correct copy of my public comment submitted to the White House Office of Science and Technology Policy, docketed as OSTP_FRDOC_0001-0008. My comment (tracking number ljh-mm9t-ux8w) was submitted as part of a public rulemaking proceeding and is publicly accessible on regulations.gov. I also filed a copy of my OSTP complaint to the Ninth Circuit docket on May 12 2025 at Dkt. 19.3 in Case No. 25-2028 and Apple would have been served a copy of that filing. ("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… 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." at p. 31). [live gov URL: https://www.federalregister.gov/documents/2023/05/03/2023-09353/request-for-information-automated-worker-surveillance-and-management] [live URL of copy of OSTP complaint: https://www.ashleygjovik.com/uploads/1/3/7/0/137008339/ostp_gjovik_comment_2023_filed_opt.pdf].

14. Attached hereto **Exhibit M** as is a true and correct copy of the Government Accountability Office Report GAO-24-107639, published August 28, 2024 and blog post published October 29, 2024, which references my public comment OSTP_FRDOC_0001-0008 in its findings (regarding all of the designations Apple claims are secret and confidential in the motion at Dkt. 294). The GAO report is publicly available at gao.gov [live URL: https://www.gao.gov/assets/gao-24-107639.pdf] and the blog post at [https://www.gao.gov/blog/why-do-i-feel-somebodys-watching-me-workplace-surveillance-can-impact-more-just-productivity]. I also published a blog post on my website about this on Aug. 28 2024 titled "*U.S. GAO Releases Report on Employer Digital Surveillance, Referencing my Comments about Apple*" [live URL: https://www.ashleygjovik.com/blog/2024-us-gao-releases-report-on-employer-digital-surveillance-referencing-my-comments-about-apple].
15. Attached hereto as **Exhibit N** is a true and correct copy of the NLRB National Settlement Agreement, Case No. 32-CA-284428, dated April 3, 2025, previously filed in this litigation as Dkt. 194. This settlement was approved by the NLRB Regional Director and posted by Apple on its internal intranet pursuant to Apple's compliance obligations under the agreement. This was filed to Dkt. 203 on April 15 2025 in this case.
16. Attached hereto as **Exhibit O** is a true and correct copy of the filing confirmation for OHRP Complaint No. 00709517, submitted March 11, 2026 to the Office for Human Research Protections, U.S. Department of Health and Human Services, concerning Apple's federally registered human subjects study NCT04196595.
17. Attached hereto as **Exhibit P** is a true and correct copy of my privacy invasion complaints to the FTC (Report Number: 154835129) on April 1 2022 and docketed with a report number by FTC around Dec. 30 2022.
18. Attached hereto as **Exhibit Q** is a true and correct copy of the complaints and communications

with German and French privacy compliance authorities regarding my complaints about Apple's "studies" and privacy-related labor law violations.

EXHIBITS — CORRESPONDENCE AND DESIGNATIONS

19. Attached hereto as **Exhibit R** is a true and correct copy of the email exchange between myself and counsel for Defendant dated February 4, 2026, including my detailed challenge to Defendant's deposition designations at issue in motion Dkt. 294 where I inform the Defendant I believe their designations are literally illegal and if they do not withdraw them, I will file an NLRB charge about it, which I did.
20. Attached hereto as **Exhibit S** is a true and correct copy of my blog post titled ***"Apple Claims It Owns Its Employees' Cervical Mucus,"*** published February 16, 2026, the same day I filed NLRB Charge No. 32-CA-381277.
21. Attached hereto as **Exhibit T** is a true and correct copy of some or all of the social media posts in question, published in Feb. of 2026.

ADDITIONAL FACTS

23. To my recollection, I never participated in Apple's ovulation study or menstruation study and I declined Apple's requests to participate. The knowledge I possess regarding those studies derives entirely from Apple's requests directed to me, my coworkers complaints, public statements and marketing including by Apple itself, and from my workplace complaints about Apple's requests.
24. I've been organizing with other Apple employees and contractors for years around Apple's data collection, studies, and concerns about invasion of privacy for both employees and the public. Another Apple privacy whistleblower, Thomas , wrote a Declaration for this case in 2024 and it is attached as ***Exhibit: Declaration of Thomas le Bonniec*** (25-2028, Dkt. 19-3, May 12 2025).
25. The content Apple designated as confidential (including the terms ovulation, cervical mucus, mucus secretions, menstruation, co-sleepers, and sexual partners) describes my own bodily experiences and my own workplace complaints. I possessed this knowledge before, during, and independent of any discovery process in this litigation. The subject of my testimony was complaining about invasion of privacy and exercising my own right to privacy/autonomy of my own body and the bodies of my coworkers.
26. Apple never designated a single produced document as confidential under the Protective Order. Apple confirmed this in writing on February 6, 2026. *See* Exhibit R.
27. Apple filed this motion on February 26, 2026, in defiance of Judge Westmore's February 20, 2026

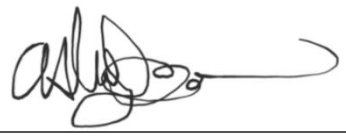
oral order requiring the parties to complete meet-and-confer before filing any motion practice.

28. I am currently in bankruptcy, insolvent, have no medical insurance, have no long-term housing, am living in a motel paid for by donations from the public, and am struggling to survive. Apple's barrage of motions, allegations, and unnecessary work meant that I was able to even sleep or complete my basic day-to-day requirements while I dropped everything to deal with Apple's latest illegal outburst. I honestly believe what Apple is doing, has been doing, and indicates it plan to do regarding this matter is extremely unlawful, contrary to public policy, and done with improper objectives including anticompetitive conduct and a reckless disregard for the law.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on March 13, 2026, in San Jose, California.

Respectfully submitted,



/s/ Ashley M. Gjovik
Ashley Gjovik (Plaintiff/*In Propria Persona*)
Filed March 13 2026 in San José, California
(415) 964-6272
ashleymgjovik@protonmail.com
2108 N. St. Ste. 4553, Sacramento, CA 95816

A. EXHIBIT A: THE VERGE

Article was filed on Dec. 25 2023 to Dkt. 35-12, at pp. 34-41 in this case's docket.

The Verge: "*Apple Cares about Privacy Unless You Work at Apple*" (Aug. 30 2021).

B. EXHIBIT B: DER SPIEGEL

Exhibit B:
DER SPIEGEL, "*Apple lädt Mitarbeiter zu Datenparty – um Gesichter zu scannen*,"
June 24 2022.

Unternehmen drohe ein Bußgeld von bis zu 50 000 Euro.

Und: »Wenn die Firmen ihr Verhalten nicht ändern, handeln sie vorsätzlich.« Sogar eine Strafverfolgung wegen Betrugs mit deutlich höheren Geldstrafen sei dann möglich.

Sämtliche Produzenten der positiv getesteten Würste bestreiten den Einsatz von Separatorenfleisch. Ein Unternehmenssprecher einer Tönnies-Tochter zweifelt die Untersuchungsmethode der Hochschule Bremerhaven an: Die vom Labor angezeigten Marker seien kein Nachweis von Separatorenfleisch, schreibt er. »In den genannten Produkten setzen wir Verarbeitungsfleisch von jungem Geflügel ein. Dies kann zu einem geringen Teil auch Knorpelzellen enthalten.«

Dagegen spricht: Die Methode springt auf einen geringen Anteil des Knorpel-Markers Kollagen II Alpha I gar nicht an.

Eine von Wiesenhof beauftragte Anwaltskanzlei schickte eidesstattliche Versicherungen der Geschäftsführer betroffener Fabriken, dass man kein Separatorenfleisch einsetze, was sich auch mit den regelmäßig selbst durchgeführten Kontrollen auf Basis amtlich anerkannter histologischer Untersuchungen und mit Überprüfungen des Kalziumgehaltes beweisen ließe.

Bei Wittkes Methode handle es sich »lediglich um einen neuen wissenschaftlichen Ansatz, ... der in der Praxis bisher jedoch keine Anwendung gefunden hat« und amtlich noch nicht anerkannt sei, schreibt die Kanzlei. Kollagene seien auch in anderen Körperteilen zu finden, insbesondere Sehnen. Außerdem sei das Verfahren bislang nur für Hähnchenfleisch entwickelt und nicht für Putenfleisch, der Hauptkomponente der Wiesenhof-Wurst.

Tatsächlich beinhalten sämtliche positiv getesteten Produkte auch Hähnchen. Und Sehnen enthalten laut einer Studie der Universität Lyon zwar Kollagene – nicht aber das spezifische Eiweiß Kollagen Typ II alpha 1, auf das die Laboruntersuchungen zielen.

Kontrollbehörden sind von dem neuen Prüfverfahren jedenfalls angetan, es könnte sich bald weiter durchsetzen und neue Erkenntnisse bringen. »Die Methode ist für uns sehr zukunftsweisend«, sagt Matthias Denker, Dezernatsleiter des Landesamts für Lebensmittelsicherheit in Mecklenburg-Vorpommern. Die nötige Ausstattung sei in amtlichen Laboren vorhanden; Lebensmittelkontrolleure könnten die Methode in ihrem Prüfalltag wohl nutzen.

Forscher Wittke gibt sich damit nicht zufrieden. Künftig will er – gefördert durch das Bundeswirtschaftsministerium – auch Separatorenfleisch anderer Tiere in Wurst aufspüren, insbesondere beim Schwein, dem meistverkauften Fleisch hierzulande.

Könnte sein, dass sich deutsche Wurstfabrikanten bald ein neues Geschäftsmodell suchen müssen.

Claus Hecking, Anne Martin, Leonie Voss, Carolin Wahnbaeck ■



Apple-Chef Cook

Brooks Kraft / Apple inc.

iPhone is watching you

TECHKONZERNE Die Whistleblowerin Ashley Gjøvik hat aufgedeckt, dass Apple heimlich aufgenommene Fotos seiner Beschäftigten nutzt, um die Gesichtserkennung auf iPhones zu trainieren. Jetzt will sie nachlegen.

Die Mail kam Ashley Gjøvik sofort eigenartig vor: An einem Augusttag vor fünf Jahren erhielt die Apple-Projektmanagerin eine Einladung zu einer »Data Collection Social Hour«. Die Party sollte gegenüber von Apples Ufo-artigen Zentrale im kalifornischen Cupertino stattfinden.

Ihr Kollege aus dem Team für Nutzerstudien versprach Getränke, Musik und »20 Minuten Datensammlung in sozialer Umgebung«. Teilnehmen durften nur fest angestellte Mitarbeiterinnen und Mitarbeiter, die »nicht empfindlich auf Licht reagieren«, so stand es in seiner Mail. Wirklich freiwillig habe sich das Event nicht angefühlt, erzählt Gjøvik heute. Sie ging hin, weil das erwartet wurde. Ihre Chefs hätten oft Druck auf sie ausgeübt, eine Teamplayerin zu sein.

Was Gjøvik damals erlebte, löste im vergangenen Sommer einen der größten Datenskandale im Apple-Reich aus. Denn sie entschloss sich, nicht über ihre Erkenntnisse zu schweigen: Der Konzern nutzt unbemerkt aufgenommene Fotos seiner Beschäftigten, um seinen Algorithmus zu trainieren. Gjøvik wurde zur Whistleblowerin – mit einer Mission, die inzwischen auch nach Europa reicht.

Dass Datenschützer aus Deutschland vielleicht bald gegen den wertvollsten Technologiekonzern der Welt vorgehen, hat mit Gjøvik zu tun.

Die 35-Jährige erzählt ihre Geschichte auf einer Parkbank in Santa Clara im Silicon Valley, ein paar Meilen von Cupertino entfernt. Bei Apple arbeitet Gjøvik heute nicht mehr, der iPhone-Konzern hat sie im Streit um die Schnüffel-App im vergangenen September entlassen. Für Apples Geschmack hatte Gjøvik zu viel preisgegeben. Auf Anfrage wollte sich der Konzern zu den Vorwürfen nicht äußern.

An die Datensammelaktion von damals erinnert sich Gjøvik so: Statt einer Party sei da ein Parkplatz gewesen, auf dem zwei Reihen schwarz verkleideter Stahlzäune standen, drei Meter hoch. Bewacht wurde der Ort von Sicherheitskräften und Kameras. An der Bar bediente ein misslauniger Mitarbeiter im Hawaii-Hemd, ein anderer führte Gjøvik und vier andere Apple-Beschäftigte an einen Klapptisch und erklärte ihnen ihre Aufgabe: Selfies machen.

Sie unterschrieb eine digitale Einverständniserklärung, von der sie nie eine Kopie bekam. Dann habe jeder das neue, noch nicht veröffentlichte iPhone-Modell X erhalten, darauf installiert eine App, die damals noch »Gobbler« hieß. Auf Deutsch »Verschlinger«. Erst später änderte Apple den Namen in einen weniger drastischen: »Glimmer«.

So hätten sie bei knapp 40 Grad in der brütenden Sonne gesessen und sich schwitzend selbst fotografiert, berichtet Gjøvik. Von oben, von der Seite, mit Sonnenbrille oder eine Grimasse schneidend. Die Kamera und mehrere Sensoren nahmen biometrische Bilder auf, in denen Gesichter dreidimensional vermessen werden, um einen Nutzer auch mit glänzender Stirn und in gleißendem Sonnenlicht zu erkennen.

Zweck der Übung: Die Apple-Mitarbeiter sollten den Algorithmus hinter Face ID füttern. Das Feature, ein Telefon über eine Gesichtserkennung zu entsperren, sollte ein paar Monate später auf dem nächsten iPhone-Modell eingeführt werden. Heute ist es von Apples Smartphones nicht mehr wegzudenken. Verbessert wird die Technik seit Jahren auch von Apple-Mitarbeitern wie Gjøvik: unfreiwillig und mit unbemerkt geschossenen Bildern aus intimsten Alltagssituationen. Im vergangenen August hatte die Whistleblowerin auf die Vorgänge aufmerksam gemacht, als sie ein Video und jene Bilder twitterte, die die Glimmer-App aufgenommen hatte.

Für Apple ist das mehr als peinlich. Keiner der großen Technologiekonzerne hat sich so sehr dem Datenschutz verschrieben wie der iPhone-Hersteller. Tim Cook, Apples sonst eher sanftmütiger Chef, attackiert regelmäßig Datenkraken wie Meta oder Alphabet und setzt sich gern demonstrativ von zweifelhaften Praktiken der Branche ab: Mit strengeren Privatsphäre-Regeln auf Apple-Geräten hat Cook fast eigenhändig Metas Wachstum abgewürgt, indem er den Hunderten Millionen iPhone- und iPad-Nutzerinnen und -Nutzern im vergangenen Jahr die Möglichkeit gab zu untersagen, dass andere Anbieter ihr Verhalten zu Werbezwecken nachverfolgen. Meta, das zu der Zeit noch Facebook hieß, warnte seine Investoren vor möglichen negativen Folgen für das Geschäft, und tatsächlich brach die Aktie wenig später ein.

Cook gibt sich stets, als ginge es ihm um Höheres und als sei in seinem eigenen Konzern alles anders: »Wenn wir anfangen, uns permanent überwacht zu fühlen, verändert sich unser Verhalten«, sagte er neulich auf einer Konferenz des »Time«-Magazins. »Wir fangen an, weniger zu tun. Weniger nachzudenken.«

Gjøvik will jetzt offenlegen, dass das Unternehmen nicht nur seine Versprechen bricht, sondern möglicherweise auch geltendes Recht. Sie hat gerade ihr Jura-Examen bestanden und arbeitet inzwischen bei einer Nichtregierungsorganisation, die gegen Zensur in China kämpft. Fertig ist sie mit Apple aber noch nicht. Wegen der Verletzung ihrer Privatsphäre ist sie mit Kaliforniens Datenschutzbehörde in Kontakt, deutsche Behörden sind ebenfalls eingeschaltet.

»Was Apple mir angetan hat, könnten sie auch deutschen Mitarbeitern (und ihren Familien und Freunden) antun oder schon angetan haben«, schreibt Gjøvik in einer E-Mail an den Bundesdatenschutzbeauftragten, die dem SPIEGEL vorliegt. Dieser hat den Fall inzwischen seinem bayerischen Kollegen weitergegeben, der zuständig ist. Apples Deutschlandzentrale sitzt in München – und forscht hier unter anderem an Bilderkennung und Anwendungen wie Face ID.

»Alle Daten, die eure Gesichter im Bild haben, sind gute Daten.«

Mail eines Studienleiters an Apple-Beschäftigte

Laut der Arbeitsrechtlerin Annegret Balzer könnte dadurch ein Datenschutzverstoß vorliegen, wenn fotografierte Personen nicht wussten, dass sie aufgenommen wurden oder durch das Abhängigkeitsverhältnis zu ihrem Arbeitgeber nicht wirklich freiwillig mitgemacht haben: Fehle eine informierte und ausdrückliche Einwilligung der Benutzer für die Gesichtserkennung, »ist eine Verarbeitung kaum vorstellbar und wäre damit rechtswidrig«.

Auch eine Geldstrafe in Millionenhöhe wäre dann möglich. Für einen Konzern mit mehr als 200 Milliarden Dollar Cashreserven wäre auch das kaum ein Problem. Doch infrage steht, ob Apple nur dann das Hohelied der Privatsphäre predigt, wenn es seinen Konkurrenten schadet.

Wie heikel der Einsatz von Glimmer außerhalb der USA ist, scheint Apple durchaus bewusst zu sein: Im August 2017 schrieb der Leiter der Studie in einer Mail an Teilnehmer, dass Mitarbeiter aus Frankreich und Deutschland ausgeschlossen seien. Eine solche Nutzerstudie würde nach dortiger Rechtslage immer als Zwang interpretiert, erklärte er später in einem LinkedIn-Post.



Juristin Gjøvik

Dann Tuffs / mauritius images / Alamy

Einen Monat nach der Parkplatzparty erhielt Gjøvik ein iPhone X, auf dem sie – im Apple-Sprech – »leben« sollte. Apple-Mitarbeiter seien grundsätzlich angehalten, die eigenen Produkte ständig im Alltag zu testen, sagt Gjøvik.

Zur Verbesserung der Gesichtserkennung fotografierte die Glimmer-App ihre Nutzer über Jahre permanent und automatisch, sobald sie das Gerät in die Hand nahmen. »Alle Daten, die eure Gesichter im Bild haben, sind gute Daten«, instruierte der Studienleiter die Teilnehmer. Der Algorithmus sei »datenhungrig«. Die Mitarbeiter sollten die Selfie-Routine als Spiel sehen: Wer 100 Bilder pro Tag oder 2000 im Monat hochlud, bekam einen virtuellen Orden.

Ende 2020 prahlte der Studienleiter in einem Blogbeitrag, Apple habe für den Start von Face ID eine Milliarde Bilder gesammelt. Gjøvik glaubt, Apple sei einfach zu geizig gewesen, ausschließlich externe Probanden für die Aufgabe zu bezahlen.

Rund vier Jahre lang fotografierte die App sie im Halbschlaf oder auf der Toilette, selbst Nacktbilder von ihr seien gespeichert gewesen. Hunderte Bilder, schätzt sie, habe die App pro Tag aufgenommen. Die, die Gjøvik öffentlich teilen will, zeigen, wie zufällig die App Schnappschüsse ihres Privatlebens aufnahm: Mal ein halber Kopf, mal mit Maske, mal sieht man weit in ihr Wohnzimmer hinein. Dass Glimmer auch Freunde, Geschwister oder Wildfremde fotografiert, die dem nie zugestimmt haben, sei kaum zu verhindern, sagt Gjøvik.

Sie habe aus der Studie nur noch rausgewollt, sich aber nicht getraut zu fragen. »Apples Kultur der Geheimnistuerei sickert tief ins Bewusstsein ein. Du hast Angst, selbst mit Behörden über offensichtliches Fehlverhalten zu reden.«

Wie wichtig es Apple war, das Programm geheim zu halten, lernte Gjøvik, nachdem sie die umstrittenen Glimmer-Aufnahmen veröffentlicht hatte. Einige Wochen später erhielt sie ein Schreiben eines von Apple beauftragten Anwalts, der sie aufforderte, die Tweets zu löschen.

Im September feuerte Apple sie nach sechseinhalb Jahren im Unternehmen. Gjøvik habe mit der Veröffentlichung der Bilder ihre Vertraulichkeitsverpflichtung gebrochen, argumentierten Apples Anwälte im März in einer Stellungnahme an das Whistleblower-Programm des US-Arbeitsministeriums. Sie liegt dem SPIEGEL vor. Gjøviks Anwalt hält dagegen, Apple halte kein Urheberrecht an Bildern von Gjøvik.

Gegen ihre Kündigung kämpft sie nun vor dem nationalen Arbeitsschutzgremium NLRB. Auch die Börsenaufsicht SEC interessiert sich nach SPIEGEL-Informationen dafür, ob Apple eine Whistleblowerin kaltstellen wollte.

Solche Verfahren ziehen sich oft lange hin. Nur eine Trennung ging ganz schnell: Gjøvik hat jetzt ein Android-Smartphone.

Patrick Beuth, Alexander Demling ■



Foto: Brooks Kraft / Apple Inc.

»20 Minuten in sozialer Umgebung«

Apple lädt Mitarbeiter zu Datenparty – um Gesichter zu scannen

Whistleblowerin Ashley Gjovik bringt Apple in Bedrängnis: Sie hat aufgedeckt, wie der Konzern Fotos von Beschäftigten sammelte, um die Gesichtserkennung im iPhone zu trainieren. Sie schaltete auch deutsche Behörden ein.

Von **Alexander Demling** und **Patrick Beuth**
24.06.2022, 14.51 Uhr • aus **DER SPIEGEL 26/2022**

Artikel zum Hören • 10 Min
Einen Monat für 1 Euro
Testen ›

Für nur 1 Euro erhalten Sie einen Monat Zugriff auf alle Artikel und jeden

(30 of 67), Page 30 of 67, Case: 25-2028, 05/20/2025, DktEntry: 27.5, Page 30 of 67
Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 15 of 217
AI Translation by DeepL

Companies could face a fine of up to 50,000 euros.

And: "If the companies do not change their behavior, they are acting intentionally." Even prosecution for fraud with significantly higher fines is then possible.

All producers of the sausages that tested positive deny the use of se- parator meat. A company spokesman for a Tönnies subsidiary questions the testing method used by the Bremerhaven University of Applied Sciences: The markers indicated by the laboratory are not evidence of mechanically recovered meat, he writes. "We use processed meat from young poultry in the products mentioned. This may also contain a small proportion of cartilage cells."

One argument against this is that the method does not respond at all to a small proportion of the cartilage marker collagen II alpha I.

A law firm commissioned by Wiesenhof sent affidavits from the managing directors of the factories concerned stating that they did not use mechanically recovered meat, which could also be proven by the regular checks they carried out themselves on the basis of officially recognized histological examinations and by checking the calcium content.

Wittke's method is "certainly a new scientific approach ... which has not yet been used in practice" and is not yet officially recognized, the law firm writes. Collagens are also found in other parts of the body, in particular the eyes. Furthermore, the process has so far only been developed for chicken meat and not for turkey meat, the main component of the Wiesenhof sausage.

In fact, all products that tested positive also contain chicken. And according to a study by the University of Lyon, tendons do contain collagens - but not the specific protein collagen type II alpha 1, which is the target of the laboratory tests.

Inspection authorities are certainly impressed by the new testing method, which could soon become more widespread and provide new insights. "The method is very forward-looking for us," says Matthias Denker, Head of Department at the State Office for Food Safety in Mecklenburg-Western Pomerania. The necessary equipment is available in official laboratories; food inspectors could well use the method in their day-to-day testing.

Researcher Wittke is not satisfied with this. In the future - with funding from the Federal Ministry of Economics - he also wants to detect cuttlefish meat from other animals in sausages, especially pork, the most commonly sold meat in this country.

It could be that German sausage manufacturers will soon have to look for a new business model.

Claus Hecking, Anne Martin, Leonie Voss, Carolin Wahnbaeck ■



Apple boss Cook

Brooks Kraft / Apple Inc.

iPhone is watching you

TECH CONCERNS Whistleblower Ashley Gjøvik has revealed that Apple uses secretly taken photos of its employees to to train facial recognition on iPhones. Now it wants to follow up.

The e-mail immediately struck Ashley Gjøvik as peculiar: On an August day five years ago, the Apple project manager received an invitation to a "Data Collection Social Hour". The party was to take place opposite Apple's UFO-like headquarters in Cupertino, California.

Her colleague from the user studies team promised drinks, music and "20 minutes of data collection in a social environment". Only permanent employees who were "not sensitive to light" were allowed to take part, according to his email. The event didn't really feel voluntary, Gjøvik says today. She went because it was expected. Her bosses often put pressure on her to be a team player.

What Gjøvik experienced back then triggered one of the biggest data scandals in the Apple empire last summer. She decided not to keep quiet about her findings: The company uses unnoticed photos of its employees to train its algorithm. Gjøvik became a whistleblower - with a mission that has since spread to Europe.

The fact that data protectionists from Germany may soon be fighting the most valuable tech The world's largest logistics group has to do with Gjøvik.

The 35-year-old tells her story on a park bench in Santa Clara in Silicon Valley, a few miles from Cupertino. Gjøvik no longer works at Apple; the iPhone company fired her last September in a dispute over the snooping app. Gjøvik had revealed too much for Apple's taste. The company declined to comment on the allegations when asked.

Gjøvik remembers the data collection campaign from back then as follows: instead of a party, there was a parking lot with two rows of black-clad steel fences, three meters high. The place was guarded by security guards and cameras. At the bar, a disgruntled employee in a Hawaiian shirt served Gjøvik and four other Apple employees at a folding table and explained their task: to take selfies.

She signed a digital declaration of consent, of which she never received a copy. Then everyone received the new, as yet unreleased iPhone model X, with an app installed on it, which at the time was still in its infancy.

was called "Gobbler". In German "Verschlinger". It was only later that Apple changed the name to something less drastic: "Glimmer".

(31 of 67), Page 31 of 67, Case: 25-2028, 05/20/2025, DktEntry: 27.5, Page 31 of 67
AI Translation by DeepL Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 16 of 217

Gjøvik reports that they sat in the sweltering sun at almost 40 degrees and photographed themselves sweating. From above, from the side, wearing sunglasses or grimacing. The camera and several sensors recorded biometric images in which faces are measured three-dimensionally in order to recognize a user even with a shiny forehead and in glaring sunlight.

Purpose of the exercise: Apple employees were to feed the algorithm behind Face ID. The feature of unlocking a phone using facial recognition was to be introduced a few months later on the next iPhone model. Today, Apple's smartphones would be unthinkable without it. Apple employees such as Gjøvik have also been improving the technology for years: involuntarily and with pictures taken unnoticed in the most intimate everyday situations. Last August, the whistleblower drew attention to what was happening when she tweeted a video and the images taken by the Glimmer app.

This is more than embarrassing for Apple. None of the major technology companies is as committed to data protection as the iPhone manufacturer. Tim Cook, Apple's otherwise rather mild-mannered boss, regularly attacks data giants such as Meta or Alphabet and likes to demonstratively distance himself from the industry's two-faced practices: With stricter privacy rules on Apple devices, Cook almost single-handedly stifled Meta's growth by allowing the hundreds of millions of iPhone and iPad users last year to prohibit other providers from tracking their behavior for advertising purposes. Meta, which was still called Facebook at the time, warned its investors of possible negative consequences for the business, and the share price did indeed collapse shortly afterwards.

Cook always acts as if he is concerned with something higher and as if everything is different in his own company: "When we start to feel constantly monitored, our behavior changes," he recently said at a Time magazine conference. "We start to do less. To think less."

Gjøvik now wants to reveal that the company is not only breaking its promises, but possibly also the law. She has just passed her law exams and now works for a non-governmental organization that fights against censorship in China. But she is not finished with Apple yet. She is in contact with California's data protection authority about the violation of her privacy, and German authorities are also involved.

"What Apple did to me, they could do to German employees (and their families and friends) or have already done to them.

> "All data containing your faces in the image are good data."
>
> Mail from a study director to Apple employees

have done," writes Gjøvik in an email to the Federal Data Protection Commissioner, which is available to SPIEGEL. He has since passed the case on to his Bavarian colleague, who is responsible. Apple's German headquarters are based in Munich - where they conduct research into image recognition and applications such as Face ID, among other things.

According to employment law expert Annegret Balzer, this could constitute a breach of data protection law if the people photographed did not know that they were being recorded or did not really participate voluntarily due to their relationship of dependence on their employer: If users did not give their informed and explicit consent for facial recognition, "processing is hardly conceivable and would therefore be unlawful".

A fine in the millions would then also be possible. For a company with more than 200 billion dollars in cash reserves, this would hardly be a problem. But the question is whether Apple only preaches the song of privacy when it harms its competitors.

Apple seems to be fully aware of how sensitive the use of mica is outside the USA: In August 2017, the head of the study wrote in an email to participants that employees from France and Germany were excluded. Such a user study would always be interpreted as coercion under local law, he later explained in a LinkedIn post.


Lawyer Gjøvik

Then Tuffs / mauritius images / Alamy

One month after the parking lot party, Gjøvik received an iPhone X, which she was supposed to "live on" - in Apple parlance. Apple employees are always encouraged to test their own products in everyday life, says Gjøvik.

To improve facial recognition, the Glimmer app continuously and automatically photographed its users for years as soon as they picked up the device. "Any data that has your faces in the picture is good data," the head of the study instructed the participants. The algorithm is "data-hungry". The employees should see the selfie route as a game: Those who uploaded 100 pictures per day or 2000 per month received a virtual medal.

At the end of 2020, the head of the study boasted in a blog post that Apple had collected one billion images for the launch of Face ID. Gjøvik believes that Apple was simply too stingy to pay only external test subjects for the task.

For around four years, the app photographed her when she was half asleep or on the toilet, and even nude pictures of her were stored. She estimates that the app took hundreds of pictures a day. The ones that Gjøvik wants to share publicly show how randomly the app took snapshots of her private life: sometimes half a head, sometimes with a mask, sometimes you can see far into her living room. The fact that Glimmer also photographs friends, siblings or complete strangers who have never consented to this can hardly be prevented, says Gjøvik.

She just wanted to get out of the study, but didn't dare to ask.
"Apple's culture of secrecy seeps deep into your consciousness. You're afraid to even talk to the authorities about obvious misconduct."

Gjøvik learned how important it was for Apple to keep the program secret after she published the controversial Glimmer recordings. A few weeks later, she received a letter from a lawyer hired by Apple asking her to delete the tweets.

In September, Apple fired her after six and a half years with the company. Gjøvik had breached her confidentiality obligation by publishing the images, Apple's lawyers argued in a statement to the US Department of Labor's whistleblower program in March. It is available to SPIEGEL. Gjøvik's lawyer, on the other hand, argues that Apple holds no copyright to Gjøvik's images.

She is now fighting her dismissal before the National Labor Relations Board (NLRB). According to SPIEGEL, the SEC is also interested in whether Apple wanted to shut down a whistleblower.

Such proceedings often take a long time. Only one separation went very quickly: Gjøvik now has an Android smartphone.

Patrick Beuth, Alexander Demling ■

C. EXHIBIT C: TELERAMA

Exhibit ***"Ashley Gjøvik, lanceuse d'alerte licenciée par Apple, seule contre tous,"*** published by Telerama, a French publication, on or about March 14 2023

Ashley Gjøvik, lanceuse d'alerte licenciée par Apple, seule contre tous

La faute de cette salariée, licenciée en 2021 : avoir révélé que la firme californienne transforme ses employés en cobayes. Allant jusqu'à les traquer dans leur intimité.



Photo Pascal Perich pour Télérama

Par Olivier Tesquet

Réservé aux abonnés

Publié le 14 mars 2023 à 06:00 Mis à jour le 14 mars 2023 à 15:39

« *Respect de la vie privée, c'est ça l'iPhone »,* claironne une récente réclame d'Apple. De longue date, la marque à la pomme a construit sa réputation sur une promesse : ses appareils au design impeccable sont des doudous qui ne mouchardent pas, ceux qui les utilisent peuvent dormir sur leurs deux oreilles. C'est beaucoup moins vrai pour les salariés de l'entreprise.

Demandez à Ashley Gjøvik. Responsable du programme d'ingénierie, cette Américaine de 36 ans a été brutalement licenciée en septembre 2021. Sa faute ? Avoir révélé que, pour améliorer les fonctionnalités de ses produits, la firme de Cupertino n'hésite pas à transformer ses équipes en cobayes, soumis à une surveillance invasive et astreints au secret comme s'ils travaillaient pour un service de renseignement. À l'aide de centaines de documents confidentiels recoupés par de multiples témoignages, *Télérama* peut raconter une culture d'entreprise où le silence est une valeur cardinale et l'intimidation, une pratique déployée au plus haut niveau. Sollicitée, Apple s'est refusée à tout commentaire.

Je suis devenue révolutionnaire quand j'ai compris qu'ils se fichaient de savoir que nous pouvions mourir.

L'histoire de Gjøvik commence comme un remake d'Erin Brockovich, cette lanceuse d'alerte immortalisée au cinéma par Julia Roberts. Début 2020, en emménageant à Santa Clara, au cœur de la Silicon Valley, sa santé se dégrade. Vertiges, palpitations, saignements, vomissements… Elle s'inquiète, consulte des cohortes de médecins et finit par découvrir que son logement est construit sur un terrain rongé par les déchets toxiques. Ils sont particulièrement envahissants dans cette partie de la Californie : pendant des décennies, la production massive de semi-conducteurs a pollué les sols, chargés de solvants cancérigènes qui remontent à la surface au fil des ans. Sur son lieu de travail tout proche, au campus d'Apple, à Sunnyvale, la jeune femme ressent des symptômes similaires. Elle avise sa hiérarchie, réclame des tests.

Son insistance agace : son employeur finit par lui intimer de ne plus évoquer le problème avec ses collègues. Elle prévient l'agence américaine de protection de l'environnement. En 2021, sur la messagerie Slack, dans un canal créé par des

salariées au moment où le mouvement #MeToo percute Apple, elle mâche de moins en moins ses mots et rassemble les colères. Au premier rang desquelles le sort que le temple du cool technologique réserve à ses ouailles. *« Je suis devenue révolutionnaire quand j'ai compris qu'ils se fichaient de savoir que nous pouvions mourir »,* se souvient-elle.

Je n'ai jamais réussi à vraiment m'intégrer, ça m'a facilité la tâche au moment de tout brûler.

Gjøvik n'est pas un produit des élites technologiques californiennes, qui n'ont qu'à traverser la rue depuis le campus de Stanford pour rejoindre une multinationale offrant salaires à six chiffres et bonus confortables. Elle a vécu *« une enfance de merde »* dans une ferme en périphérie de Portland, dans l'Oregon pluvieux. Elle travaille dès 14 ans, manifeste contre la guerre en Irak à 16 et coupe les ponts avec sa famille à 20.

Après avoir débuté chez Nike *(« J'essayais de ne pas penser au travail des enfants »),* elle atterrit un peu par hasard chez Apple en 2015, fauchée et endettée. *« J'ai commencé à travailler dans la technologie parce que j'avais besoin de comprendre les systèmes complexes »,* explique-t-elle d'une voix de mitraillette rigolarde, son chien Captain sur les genoux. Elle se tue à la tâche, soixante-dix heures par semaine pendant cinq ans. Elle prend du galon, mais pas le pli de la culture locale, qui, souvent, ressemble à une expérimentation sociale en milieu clos : *« Je n'ai jamais réussi à vraiment m'intégrer, ça m'a facilité la tâche au moment de tout brûler. »*

Goûtant peu ce vent de rébellion, Apple décide de la mettre au repos forcé en août 2021, invoquant une enquête interne lancée sur la base de ses accusations. Pas refroidie, Gjøvik saisit l'agence fédérale chargée de faire respecter le droit du travail. Fin août, elle dévoile sur Twitter l'existence d'un programme clandestin, Gobbler (plus tard rebaptisé Glimmer). Déployé en 2017 auprès des salariés, cet outil interne a accompagné le lancement de Face ID, la fonctionnalité de reconnaissance faciale d'Apple, qui permet de déverrouiller son téléphone avec son visage. Dans un e-mail envoyé le 3 août 2017, et que nous avons pu consulter, un ingénieur de l'équipe vidéo explique les grandes lignes : pour entraîner l'algorithme, il faut le nourrir. Une fois activé, Gobbler prend une photo dès qu'il détecte un visage. C'est un œil qui ne cligne jamais. *« En matière de données, nous en voulons plus »,* ajoute l'ingénieur gourmand.

À lire aussi :

> De “The Social Network” à “Super Pumped”, dix films et séries qui dégomment la Silicon Valley

Dans un autre document, Apple précise quelques règles. L’application ne peut pas être utilisée en France ou en Allemagne (elle y serait illégale du fait des réglementations locales) et les salariés sont priés de ne pas télécharger de clichés immortalisés dans des lieux intimes. Gjøvik est récalcitrante, mais pour arracher le consentement de ses cobayes, l’employeur sait ruser. Un jour d’été, elle est invitée à un *« apéro de collecte de données »* d’une vingtaine de minutes, sans plus de précisions. Interdiction d’en parler sans obtenir le feu vert du service juridique. Une fois sur place, à deux pas du siège historique de la société, elle découvre *« ce qui ressemble à un complexe militaire »* protégé par des gardes. Il faut donner son téléphone, passer une porte, la refermer, en ouvrir une autre, et pénétrer quatre par quatre dans un espace cylindrique en plein cagnard pour se faire tirer le portrait. Un vrai trombinoscope composé par la force, dont l’objectif est d’améliorer l’intelligence artificielle

Quelques jours après ses premières révélations, le 9 septembre, Apple la licencie et la convoque dans l’heure, invoquant une violation de la propriété intellectuelle de l’entreprise. Elle se retrouve dans le viseur de la *« Worldwide Loyalty Team »*, des investigateurs maison qui ont souvent fait carrière dans la police ou les services secrets. Par le passé, ces privés n’ont pas hésité à pénétrer dans des domiciles afin de retrouver un prototype d’iPhone égaré. En 2017, Apple s’est même vantée d’avoir fait arrêter douze salariés trop bavards. On ne badine pas avec les secrets industriels de la première capitalisation boursière de la planète. Dans un courrier transmis au Département du travail le 4 mars 2022, les avocats d’Apple justifient le licenciement d’Ashley Gjøvik : *« Elle a choisi de divulguer des informations qu’elle était tenue de garder confidentielles. »* Gobbler n’y est jamais nommé, la société se bornant à évoquer *« l’étude »* sous le nom de code Omega.

Au fil des ans, Apple a multiplié les expérimentations de ce type, enregistrant et stockant toutes sortes d’informations intimes et biométriques sur ses salariés-testeurs : scan des conduits auditifs pour optimiser l’ergonomie des AirPods (les designers s’enorgueillissant de posséder *« l’une des plus larges bibliothèques d’oreilles de la planète »*), mesure du sommeil, pression artérielle et même surveillance du cycle menstruel. Sous couvert d’anonymat, une ex-salariée a accepté de nous transmettre les photos d’un kit proposé par Apple en 2019 en échange d’un bon d’achat de 10 dollars, afin de mesurer la qualité des glaires cervicales de son utérus. Inquiète des conséquences d’un refus, elle a accepté de se prêter à l’exercice, qui la hante encore.

Vous ne devez avoir aucune attente en matière de vie privée lorsque vous utilisez vos appareils personnels ou ceux de quelqu'un d'autre à des fins professionnelles. Apple

Si le géant de la tech n'hésite pas à coloniser le corps de ses collaborateurs, ceux-ci sont priés de ne pas moufter. La politique interne d'Apple, elle aussi confidentielle, annonce la couleur : *« Vous ne devez avoir aucune attente en matière de vie privée lorsque vous utilisez vos appareils personnels ou ceux de quelqu'un d'autre à des fins professionnelles, lorsque vous utilisez les systèmes ou les réseaux d'Apple, ou lorsque vous vous trouvez dans les locaux d'Apple. »* Mais ça pourrait ne pas durer. Fin janvier, le gendarme du droit du travail a estimé que la politique d'omerta de l'entreprise violait la loi, ouvrant la voie à un procès. Est notamment visé un mémo intimidant envoyé par le grand patron, Tim Cook, une semaine après le licenciement de la lanceuse d'alerte. *« Nous savons que les auteurs de fuites constituent un petit nombre de personnes,* écrivait-il. *Nous savons également que les personnes qui divulguent des informations confidentielles n'ont pas leur place ici. »*

À lire aussi :

"Les désobéissants" sur France.tv : 10 récits de combats citoyens pour faire éclater la vérité

Pour l'avocat Seth Goldstein, qui a récemment aidé les travailleurs d'Amazon à combattre les pratiques antisyndicales de Jeff Bezos, c'est un signal important : *« Les révélations d'Ashley mettent en lumière le pire de la culture d'entreprise dans la Silicon Valley. J'ai bon espoir que son cas permette de faire bouger les choses, car les gens n'ont plus confiance en ces sociétés. »* La lanceuse d'alerte, elle, n'est pas près de rendre les armes, même si le combat l'a éprouvée. *« J'ai parfois l'impression d'avoir perdu mon identité, et je n'ai jamais été aussi proche du suicide depuis l'adolescence »,* explique-t-elle au bord des larmes, en ajoutant qu'elle a trouvé du réconfort dans un livre sur les blessures morales des GI de retour de guerre. Début février, elle a eu rendez-vous avec des enquêteurs de la Securities and Exchange Commission, l'autorité des marchés financiers américains. Dans la plainte qu'elle a adressée à une douzaine d'autorités judiciaires ou de protection de la vie privée, elle annonce avec une pointe d'humour sa future reconversion en droit international public, droits humains et *« méga-corporations dystopiques ».*

Ashley Gjøvik, whistleblower fired by Apple, alone against all odds

The fault of this employee, who will be dismissed in 2021: she revealed that the Californian firm turns its employees into guinea pigs. Even stalking them in their private lives.



Photo Pascal Perich pour Télérama

By Olivier Tesquet

Ashley Gjøvik, whistleblower fired by Apple, alone against all odds

Reserved for subscribers

Published on March 14, 2023 at 06:00 Updated on March 14, 2023 at 15:39

"*Respect for privacy, that's the iPhone,"* trumpets a recent Apple advert. The Apple brand has long built its reputation on one promise: its impeccably-designed devices.
are soft toys that don't snitch, so those who use them can rest easy. This is much less true for company employees.

Just ask Ashley Gjøvik. Head of the engineering program, this 36-year-old American was brutally fired in September 2021. Her fault? Revealing that, in order to improve the functionalities of its products, the Cupertino firm does not hesitate to turn its teams into guinea pigs, subjected to invasive surveillance and sworn to secrecy as if they were working for an intelligence service. With the help of hundreds of confidential documents cross-checked by multiple testimonies, *Télérama* can tell the story of a corporate culture where silence is a cardinal value and intimidation a practice deployed at the highest level. When contacted, Apple refused to comment.

I became a revolutionary when I realized that they didn't care if we died.

Gjøvik's story begins like a remake of Erin Brockovich, the whistleblower immortalized in film by Julia Roberts. In early 2020, when she moves to Santa Clara, in the heart of Silicon Valley, her health takes a turn for the worse. Vertigo, palpitations, bleeding, vomiting... She becomes worried, consults cohorts of doctors and ends up discovering that her home is built on land eaten away by toxic waste. Toxic waste is particularly pervasive in this part of California: for decades, the massive production of semiconductors has polluted the soil with carcinogenic solvents, which have surfaced over the years. At her nearby workplace, the Apple campus in Sunnyvale, the young woman experienced similar symptoms. She notified her superiors and requested tests.

Her insistence annoyed her employer, who finally told her not to raise the issue with her colleagues. She notifies the U.S. Environmental Protection Agency. In 2021, on the messaging service Slack, in a channel created by

salaried employees at a time when the #MeToo movement is hitting Apple, she's mincing her words less and less and gathering anger. Foremost among these is the fate that the temple of technological cool reserves for its flock. "*I became a revolutionary when I realized that they didn't care if we died,"* she recalls.

I never really managed to fit in, which made it easier for me when it came time to burn the place down.

Gjøvik is not a product of California's tech elites, who only have to cross the street from the Stanford campus to join a multinational offering six-figure salaries and comfortable bonuses. She has lived
She *had a "shitty childhood"* on a farm on the outskirts of Portland, in rainy Oregon. She worked from the age of 14, protested against the war in Iraq at 16 and cut ties with her family at 20.

After starting out at Nike *("I was trying not to think about child labor"),* she landed somewhat by chance at Apple in 2015, broke and in debt. *"I started working in technology because I needed to understand complex systems,"* she explains in a laughing machine-gun voice, her dog Captain on her lap. She worked herself to the bone, seventy hours a week for five years. She grew in stature, but not in the local culture, which often resembled a social experiment in a closed environment: *"I never really managed to fit in, which made it easier for me when it came time to burn the place down.*

Tasting little of this wind of rebellion, Apple decided to put her on forced rest in August 2021, citing an internal investigation launched on the basis of her accusations. Undaunted, Gjøvik took her case to the federal agency responsible for enforcing labor law. At the end of August, she revealed on Twitter the existence of a clandestine program, Gobbler (later renamed Glimmer). Deployed to employees in 2017, this internal tool accompanied the launch of Face ID, Apple's facial recognition feature, which allows you to unlock your phone with your face. In an e-mail sent on August 3, 2017, and which we were able to consult, an engineer from the video team explains the broad outlines: to train the algorithm, you have to feed it. Once activated, Gobbler takes a photo as soon as it detects a face. It's an eye that never blinks. "*When it comes to data, we want more,"* adds the greedy engineer.

Read also:

> From "The Social Network" to "Super Pumped", ten films and series that put Silicon Valley to shame

In another document, Apple specifies a few rules. The application cannot be used in France or Germany (it would be illegal there due to local regulations), and employees are asked not to download snapshots taken in intimate places. Gjøvik is recalcitrant, but to obtain the consent of her guinea pigs, the employer knows how to trick them. One summer day, she is invited to a 20-minute *"data collection aperitif"*, with no further details. She was forbidden to talk about it without a green light from the legal department. Once on site, a stone's throw from the company's historic headquarters, she discovers *"what looks like a military complex"* protected by guards. You have to hand over your phone, pass through a door, close it again, open another, and enter four by four into a cylindrical space in the middle of a hot summer to have your portrait taken. A real trombinoscope composed by force, with the aim of improving artificial intelligence.

A few days after her first revelations, on September 9, Apple fired her and summoned her within the hour, citing a violation of the company's intellectual property. She found herself in the crosshairs of the *Worldwide Loyalty Team*, in-house investigators who often had careers in the police or secret services. In the past, these privates have not hesitated to enter homes in order to track down a misplaced iPhone prototype. In 2017, Apple even boasted of having twelve overly talkative employees arrested. be trifled withThe industrial secrets of the world's largest market capitalization are not to . In a letter sent to the Department of Labor on March 4, 2022, Apple's lawyers justify Ashley Gjøvik's dismissal: *"She chose to disclose information that she was required to keep confidential."* Gobbler is never named, the company merely referring to *"the study"* under the code name Omega.

Over the years, Apple has multiplied experiments of this kind, recording and storing all kinds of intimate and biometric information on its employee-testers: ear canal scans to optimize AirPods ergonomics (the designers boast *"one of the largest ear libraries on the planet"*), sleep measurements, blood pressure and even menstrual cycle monitoring. On condition of anonymity, a former employee agreed to send us photos of a kit offered by Apple in 2019 in exchange for a $10 voucher, to measure the quality of cervical mucus in her uterus. Worried about the consequences of refusal, she agreed to take part in the exercise, which still haunts her.

You should have no expectation of privacy when using your personal devices or someone else's for business purposes. Apple

If the tech giant doesn't hesitate to colonize the bodies of its employees, the latter are asked not to squawk. Apple's internal policy, also confidential, announces the color: *"You should have no expectation of privacy when using your personal devices or anyone else's for business purposes, when using Apple systems or networks, or when on Apple premises."* But it might not last. At the end of January, the labor law watchdog ruled that the company's omerta policy violated the law, paving the way for a lawsuit. At issue is an intimidating memo sent by CEO Tim Cook a week after the whistleblower's dismissal. *We know that leakers are a small number of people,"* he wrote. *We also know that people who disclose confidential information have no place here."*

> **Read also:**
>
> "Les désobéissants" on France.tv: 10 stories of citizens' struggles to get the truth out

For attorney Seth Goldstein, who recently helped Amazon workers fight Jeff Bezos' anti-union practices, this is an important signal: *"Ashley's revelations highlight the worst of corporate culture in Silicon Valley. I'm hopeful that her case will help shake things up, because people no longer trust these companies."* As for the whistleblower, she's not about to give up, even if the battle has taken its toll on her. "*I sometimes feel like I've lost my identity, and I've never been so close to suicide since I was a teenager,"* she explains, on the verge of tears, adding that she has found solace in a book about the moral wounds of GIs returning from war. In early February, she had an appointment with investigators from the Securities and Exchange Commission. In the complaint she sent to a dozen judicial and privacy protection authorities, she humorously announces her future reconversion to public international law, human rights and the protection of privacy. *"dystopian megacorporations".*

D. EXHIBIT D: TELEGRAPH

Exhibit ***Apple whistleblower brings spying claims to UK: Data watchdog opens investigation into privacy accusations against iPhone maker,"*** published by The Telegraph on or about April 10 2022

The Telegraph

Apple whistleblower brings spying claims to UK

Data watchdog opens investigation into privacy accusations against iPhone maker

By Lucy Burton, EMPLOYMENT EDITOR

10 April 2022 • 9:00am

Britain's information watchdog is investigating claims that Apple was able to access personal information on workers' phones after a privacy complaint was lodged by a whistleblower.

Ashley Gjøvik, a former senior Apple engineer, has filed a 54-page privacy complaint against the iPhone maker alleging unlawful data collection and invasion of employee privacy over "years and multiple countries".

In the filing, which has been lodged with the UK Data Protection Information Commissioner's Office (ICO) and its counterpart in Brussels, Ms Gjøvik claimed that she publicly expressed concerns about Apple "pressuring its employees to participate in invasive data collection procedures, including scans of ears/ear canals".

She also accused the company of using an app on employees' iPhones that "automatically took photos/videos whenever it 'thought it saw a face'".

In the filing Ms Gjøvik said: "I respectfully request that you investigate the matters I raised and open a larger investigation into these topics within Apple's corporate offices globally."

The complaint was also submitted to the Data Protection Commission in Ireland and London-based Big Brother Watch, the privacy campaigning organisation.

An ICO spokesman said: "We are aware of this matter and we will assess the information

provided."

Ms Gjøvik was fired by Apple last September for allegedly violating the company's rules against leaking confidential information.

She claimed to have begun raising concerns about workplace safety in March last year, including those related to Apple's policies on how it can search and surveil employees' work phones.

Ms Gjøvik has also alleged that she has faced bullying and harassment from her manager and other colleagues, in a campaign that has been dubbed Apple's "MeToo" moment.

This is thought to be the first time that she has tried to take her battle against the notoriously secretive tech giant to the UK.

The campaign dragged Apple into a growing wave of employee activism affecting its Silicon Valley rivals. In 2018, more than 20,000 Google staff held a walkout against forced arbitration agreements and alleged payouts related to sexual harassment.

An Apple spokesman said: "We are and have always been deeply committed to creating and maintaining a positive and inclusive workplace. We take all concerns seriously and we thoroughly investigate whenever a concern is raised and, out of respect for the privacy of any individuals involved, we do not discuss specific employee matters."

Business Briefing newsletter

Our daily digest packed with news and analysis



Sign up

Related Topics

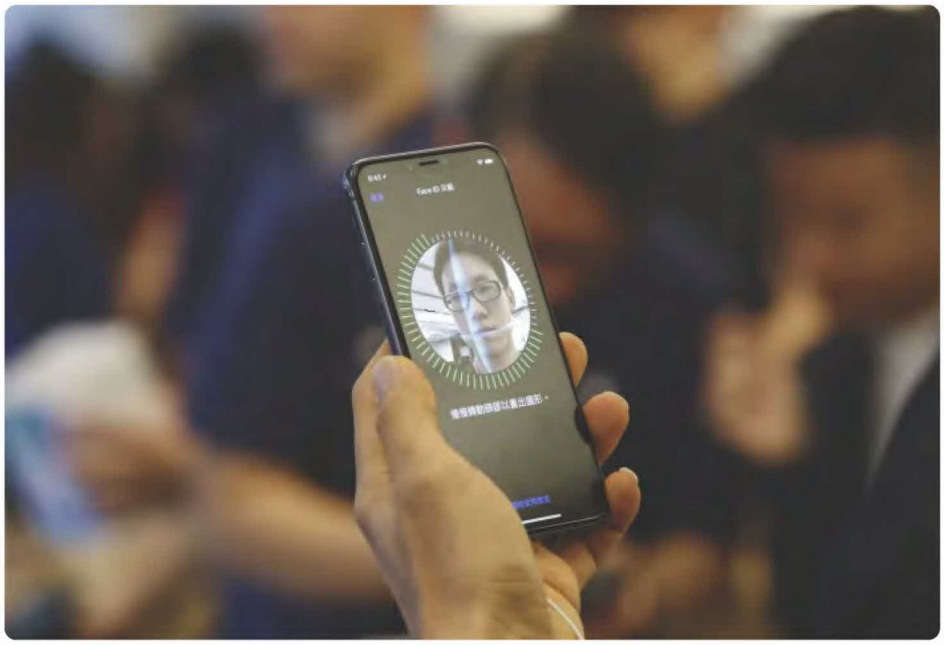
Apple, Privacy, Information Commissioner Office

E. EXHIBIT E: TECHCRUNCH

Exhibit ***Ex-Apple employee takes Face ID privacy complaint to Europe,"*** published by TechCrunch and Yahoo! News around April 11 2022,

TechCrunch

Ex-Apple employee takes Face ID privacy complaint to Europe



Natasha Lomas
Mon, April 11, 2022, 10:58 AM · 8 min read

Privacy watchdogs in Europe are considering a complaint against Apple made by a former employee, Ashley Gjøvik, who alleges the company fired her after she raised a number of concerns, internally and publicly, including over the safety of the workplace.

Gjøvik, a former senior engineering program manager at Apple, was fired from the company last September after she had also raised concerns about her employer's approach towards staff privacy, some of which were covered by the Verge in a report in August 2021.

TRENDING

Audio captures Russian soldiers discussing killing and raping Ukrainians, with one saying, 'If...
Business Insider · 2 min read

Connecticut advances death notification bill after tragic deaths of 2 Black women
Yahoo News · 4 min read

Putin's War in Ukraine Shatters an Illusion in Russia
The New York Times · 8 min read

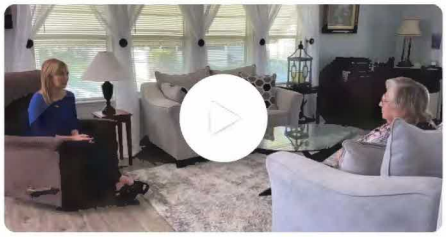
72 people at high-profile D.C. dinner test positive for Covid
NBC News · 3 min read

How did quarterback Dwayne Haskins die on a South Florida highway? Here's what we know.
Miami Herald · 1 min read

POPULAR



Employee experience is as strong as ever at the 100 Best Companies
Fortune



Moving to Florida? New Florida residents rack up complaints against moving companies
WFTS-Tampa

HOME MAIL NEWS FINANCE SPORTS ENTERTAINMENT MORE SEARCH SHOPPING YAHOO PLUS Download the Yahoo News app
yahoo!news Sign in Mail
News US Politics World COVID-19 Climate Change Originals Health Science Podcasts Contact Us Videos

At the time, Gjøvik had been placed on administrative leave by Apple after raising concerns about sexism in the workplace, and a hostile and unsafe working environment which it had said it was investigating. She subsequently filed complaints against Apple with the US National Labor Relations Board.

Those earlier complaints link to the privacy complaint she's sent to international oversight bodies now because Gjøvik says she wants scrutiny of Apple's privacy practices after it formally told the US government its reasons for firing her -- and "felt comfortable admitting they'd fire employees for protesting invasions of privacy", as she puts it -- accusing Apple of using her concerns over its approach to staff privacy as a pretext to terminate her for reporting wider safety concerns and organizing with other employees about labor concerns.

The UK's Information Commissioner's Offie (ICO) and France's CNIL both confirmed receipt of Gjøvik's privacy complaint against Apple.

A spokesperson for the ICO told TechCrunch: “We are aware of this matter and we will assess the information provided.”

France's CNIL also sent confirmation that it's looking at Gjøvik's complaint.

"We have received this complaint which it is currently being investigated," a CNIL spokesperson told us, adding: "I cannot communicate any further details at this time."

The development was first covered by the Telegraph -- which reported yesterday that it's thought to be the first time Gjøvik has sought to press her privacy complaint against Apple in the UK.

Story continues

Why Apple Stock Is Falling Today
Motley Fool



Exclusive-Apple faces extra EU antitrust charge in music streaming probe -source
Reuters



Rebuttal: Bill protects online privacy, security
Palm Beach Daily News

GALLUP EXCEPTIONAL WORKPLACE AWARD
2022 WINNER

Regions Bank Wins Gallup Exceptional Workplace Award
News Direct



Here are the Fortune 100 Best Companies to Work For® in 2022, according to nearly 1 million employees
News Direct

RECOMMENDED STORIES

F. EXHIBIT F: GIZMODO

Exhibit F: Article posted at Dkt. 35-12 on Dec. 25 2023 at pp. 80-93

Gizmodo, "*Apple Wanted Her Fired. It Settled on an Absurd Excuse The reasons for firing Ashley Gjøvik include tweeting a photo of herself—taken by her own phone,"* Oct. 15 2021.

G. EXHIBIT G: INVERSE

Exhibit G: Article posted at Dkt. 35-12 on Dec. 25 2023 at pp. 94-96.

Inverse, "*Apple is leaning on weak arguments to defend a senior engineer's firing*," Oct. 15 2021.

H. EXHIBIT H: BIOMETRIC UPDATE

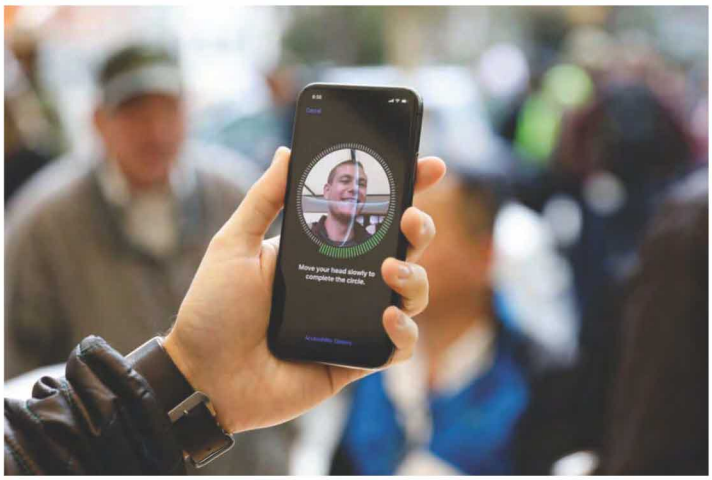
Exhibit Biometric Update article titled "***Ex-employee accuses Apple of training iPhone biometrics by violating staff privacy,"*** and published around April 20 2022.

Share
Tweet
Link
Comment

Ex-employee accuses Apple of training iPhone biometrics by violating staff privacy

Apr 20, 2022, 6:51 pm EDT | Chris Burt

CATEGORIES Biometric R&D | Biometrics News | Mobile Biometrics



Apple was questioned about where it collected the 1 billion images it trained the Face ID biometric algorithm with by a member of U.S. Congress back in 2017, but no direct answer was offered. Now, an ex-employee of the company is taking it to court in Europe over sourcing those training images from its staff, The Telegraph reports.

Minnesota Senator Al Franken requested information on a range of points when Apple first introduced face biometrics to the iPhone X, some but not all of which was provided in the company's response.

Former Apple employee Ashley Gjøvik was placed on administrative leave after complaining to the company about a sexist work environment, and then was fired, she says for raising concerns about violations of staff privacy. She has also filed a complaint with the National Labor Relations Board in the U.S.

The company invited its employees to participate in product testing, and sometimes to have their biometrics collected, but Gjøvik says the testing and collection seemed to be mandatory. She describes the use of Apple's internal Gobbler app (later called Glimmer) to upload personal data employees had collected to company servers, and directly claims that employee data is the source of the billion images used to train Face ID.

MOST READ THIS WEEK

Stakeholders review Ethiopia's proposed digital ID legislative framework

Biometrics partnerships set up billions in revenues forecast by analysts

Biden urged to consider federal digital identity framework

Biometrics secure UNHCR direct cash payments to Ukrainian refugees

UK government opens bid for mobile fingerprint biometric enrollment devices

It's fun. It's trendy. It's putting your iris biometrics on the market for free

GSA finds 'bias' in facial recognition errors, plans tests but no deployment

Paravision and HID Global co-developing new line of face biometric solutions

iProov brings counter-suit against FaceTec in biometric liveness IP dispute

Biometrics capture with feature phones to boost Africa's financial inclusion

Daily Biometrics News

FEATURED COMPANY

Daon

France's data protection authority CNIL and the UK's Information Commissioner's Office have each confirmed that they are investigating the allegations, according to TechCrunch, and other regulators are listed in the complaint but have not confirmed investigations.

Ultimately, Gjøvik is alleging non-disclosure agreements and employee privacy policies that do not meet legal standards.

Controversy around the origin of biometric training data has led to lawsuits and recent ethical commitments from biometrics developers.

Article Topics

Apple | biometric data | biometrics | data collection | data protection | face biometrics | Face ID | iPhone | privacy

Latest Biometrics News

Autoencoder approach to vein biometrics development shows promise in EAB presentation

Panel recommends non-intrusive airport biometrics for India

Chinese, U.S. researchers turn teeth-grinding into a biometric identifier

Affective computing draws Intel's attention, prompts debate

Easier and Idemia to collaborate on biometric Entry/Exit System for Lithuania

GAO says US military playing too loose with AI development management

Comments

Leave a Reply

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Subscribe To The BiometricUpdate.com Email Newsletter

Stay on the cutting edge of the biometrics industry by subscribing to daily news updates from BiometricUpdate.com

LEARN MORE



The future of identity lives here. Fast mobile authentication using your face, voice, or fingerprint? We helped invent that technology. And today, we're building even faster, safer ways to help connect your customers to the services they love, in every channel, for life.

LEARN MORE

More Biometrics Companies

BIOMETRICS RESEARCH

Expect digital ID to balloon in users and revenue by 2026: Juniper Research

Two analyses project facial recognition market at around $13B by 2028

Ponemon Institute highlights rise in authentication failure rates and related costs

More Biometrics Research

BIOMETRICS WHITE PAPERS

The validation and development of the QuantumCrypt technology

On-demand webinar – Human or machine: AI proves best at spotting biometric attacks

ID document verification impact report

More White Papers

BIOMETRICS EVENTS

ID4Africa LiveCasts: Mobile for Identity Management and Inclusive ID4D
Online: Mar 9 - Apr 27, 2022

TDK Ventures presents DX Week 2022
Online: Apr 18 - Apr 21, 2022

SECON 2022
KINTEX, Korea: Apr 20 - Apr 22, 2022

More Biometrics Events

I. EXHIBIT I:
American Journal of Obstetrics and Gynecology

Exhibit I:

Mahalingaiah, Shruthi et al. "Design and methods of the Apple Women's Health Study: a digital longitudinal cohort study." *American journal of obstetrics and gynecology* vol. 226,4 (2022): 545.e1-545.e29. doi:10.1016/j.ajog.2021.09.041, https://pmc.ncbi.nlm.nih.gov/articles/PMC10518829/

HHS Public Access
Author manuscript
Am J Obstet Gynecol. Author manuscript; available in PMC 2023 September 25.

Published in final edited form as:
Am J Obstet Gynecol. 2022 April ; 226(4): 545.e1–545.e29. doi:10.1016/j.ajog.2021.09.041.

Design and methods of the Apple Women's Health Study: a digital longitudinal cohort study

Shruthi Mahalingaiah, MD, MS,
Harvard T.H. Chan School of Public Health, Boston, MA

Victoria Fruh, PhD,
Harvard T.H. Chan School of Public Health, Boston, MA

Erika Rodriguez, MS,
Harvard T.H. Chan School of Public Health, Boston, MA

Sai Charan Konanki, MS,
Harvard T.H. Chan School of Public Health, Boston, MA

Jukka-Pekka Onnela, DSc,
Harvard T.H. Chan School of Public Health, Boston, MA

Alexis de Figueiredo Veiga, MS,
Harvard T.H. Chan School of Public Health, Boston, MA

Genevieve Lyons, MS,
Harvard T.H. Chan School of Public Health, Boston, MA

Rowana Ahmed, MS,
Harvard T.H. Chan School of Public Health, Boston, MA

Huichu Li, PhD,
Harvard T.H. Chan School of Public Health, Boston, MA

Nicola Gallagher, MS,
Harvard T.H. Chan School of Public Health, Boston, MA

Anne Marie Z. Jukic, PhD, MSPH,
Epidemiology Branch, Division of Intramural Research, National Institute of Environmental Health Sciences, National Institutes of Health, Research Triangle Park, Durham, NC

Kelly K. Ferguson, PhD, MPH,
Epidemiology Branch, Division of Intramural Research, National Institute of Environmental Health Sciences, National Institutes of Health, Research Triangle Park, Durham, NC

Donna D. Baird, PhD,
Epidemiology Branch, Division of Intramural Research, National Institute of Environmental Health Sciences, National Institutes of Health, Research Triangle Park, Durham, NC

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Corresponding author: Shruthi Mahalingaiah, MD, MS. shruthi@hsph.harvard.edu.
B.A.C., R.H., M.A.W. contributed equally to this work and share senior authorship.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Allen J. Wilcox, MD, PhD,
Epidemiology Branch, Division of Intramural Research, National Institute of Environmental Health Sciences, National Institutes of Health, Research Triangle Park, Durham, NC

Christine L. Curry, MD, PhD,
Health, Apple Inc, Cupertino, CA

Sanaa Suharwardy, MD,
Division of Maternal Fetal Medicine, Department of Obstetrics and Gynecology, Stanford University School of Medicine, Stanford, CA

Tyler Fischer-Colbrie, MBA,
Health, Apple Inc, Cupertino, CA

Gracee Agrawal, MS,
Health, Apple Inc, Cupertino, CA

Brent A. Coull, PhD,
Harvard T.H. Chan School of Public Health, Boston, MA

Russ Hauser, MD, ScD, MPH,
Harvard T.H. Chan School of Public Health, Boston, MA

Michelle A. Williams, ScD
Harvard T.H. Chan School of Public Health, Boston, MA

Abstract

BACKGROUND: Prospective longitudinal cohorts assessing women's health and gynecologic conditions have historically been limited.

OBJECTIVE: The Apple Women's Health Study was designed to gain a deeper understanding of the relationship among menstrual cycles, health, and behavior. This paper describes the design and methods of the ongoing Apple Women's Health Study and provides the demographic characteristics of the first 10,000 participants.

STUDY DESIGN: This was a mobile-application-based longitudinal cohort study involving survey and sensor-based data. We collected the data from 10,000 participants who responded to the demographics survey on enrollment between November 14, 2019 and May 20, 2020. The participants were asked to complete a monthly follow-up through November 2020. The eligibility included installed Apple Research app on their iPhone with iOS version 13.2 or later, were living in the United States, being of age greater than 18 years (19 in Alabama and Nebraska, 21 years old in Puerto Rico), were comfortable in communicating in written and spoken English, were the sole user of an iCloud account or iPhone, and were willing to provide consent to participate in the study.

RESULTS: The mean age at enrollment was 33.6 years old (±standard deviation, 10.3). The race and ethnicity was representative of the US population (69% White and Non-Hispanic [6910/10,000]), whereas 51% (5089/10,000) had a college education or above. The participant geographic distribution included all the US states and Puerto Rico. Seventy-two percent (7223/10,000) reported the use of an Apple Watch, and 24.4% (2438/10,000) consented to sensor-

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

based data collection. For this cohort, 38% (3490/9238) did not respond to the Monthly Survey: Menstrual Update after enrollment. At the 6-month follow-up, there was a 35% (3099/8972) response rate to the Monthly Survey: Menstrual Update. 82.7% (8266/10,000) of the initial cohort and 95.1% (2948/3099) of the participants who responded to month 6 of the Monthly Survey: Menstrual Update tracked at least 1 menstrual cycle via HealthKit. The participants tracked their menstrual bleeding days for an average of 4.44 (25%–75%; range, 3–6) calendar months during the study period. Non-White participants were slightly more likely to drop out than White participants; those remaining at 6 months were otherwise similar in demographic characteristics to the original enrollment group.

CONCLUSION: The first 10,000 participants of the Apple Women's Health Study were recruited via the Research app and were diverse in race and ethnicity, educational attainment, and economic status, despite all using an Apple iPhone. Future studies within this cohort incorporating this high-dimensional data may facilitate discovery in women's health in exposure outcome relationships and population-level trends among iPhone users. Retention efforts centered around education, communication, and engagement will be utilized to improve the survey response rates, such as the study update feature.

Keywords

digital health; longitudinal cohort; menstrual cycles; women's health

Introduction

Multiple factors influence the menstrual cycle length, duration of flow, and cyclicity. Common factors include stress, nutrition and body weight, physical activity, and combination lifestyle factors. Furthermore, menstrual cycle function is an indicator of health and longevity.[1] For example, bone density is built and maintained in the presence of cyclic ovarian function.[2] Fertility, terminal breast differentiation, and aspects of cognition and memory are also influenced by menstrual status and function.[3–5] The endocrine pathways involved in menstrual cycle physiology include the hypothalamic-pituitary-ovarian axis and a healthy functioning of the thyroid and adrenal glands; the anatomic structures necessary include the uterus, endometrium, and ovaries.

Furthermore, irregular patterns or the absence of menstrual cycles can serve as indicators of underlying health problems. The presence of irregular menstrual cycles may indicate hormonal disturbances, including thyroid disorders, prolactinomas, systemic illness (including cancers), anatomic pathology such as uterine fibroids, polyps, or adenomyosis; it has also has been linked to an increase in all-cause mortality.[1] Abnormalities in the bleeding length and amount affect up to 30% of those who menstruate.[6] The existing data on the menstrual cycle characteristics, including the normal distributions of the cycle length and bleeding days, are based on prior and well-designed but demographically-limited cohorts.[7,8] Little is known about how these conditions vary across subpopulations or how they relate to future health conditions. An understanding of population-based variation in menstrual cycle characteristics is lacking.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

The objectives of this study are to (1) advance the understanding of the menstrual cycle, including how it relates to exercise, sleep, environmental, behavioral, and other physiological processes, and (2) inform screening and risk assessment for gynecologic health conditions using menstrual cycle, reproductive, health, and sensor data. We present here the design of the Apple Women's Health Study (AWHS) and the characteristics of the first 10,000 participants enrolled in the study, including their follow-up after 6 months of participation.

Materials and Methods

Survey design

The survey questions for the AWHS were derived from previous, similarly large longitudinal studies on women's health. These surveys included the National Health and Nutrition Examination Survey developed by the Centers for Disease Control and Prevention, the Perceived Stress Scale, All of Us study—a large research program sponsored by the National Institutes of Health, Nurses' Health Study 2, and the Ovulation and Menstruation Health Study.[9–12] The questions were modified for a mobile user experience and were standardized across 2 other research studies also housed in the Apple Research app. For menstrual-cycle-specific questions, the exposures hypothesized to affect the hypothalamic-pituitary-ovarian axis in a cycle-specific way were included. Once the research teams had completed the initial drafting of the baseline survey, it was reviewed by Apple, Inc. to conform to their design standards across the 3 studies.

The interface for the Research app was designed to be intuitive and simple. The research profile completed at enrollment is common to all 3 studies and includes the initial demographic survey. To implement the intuitive and simple survey concept, the baseline women's health study survey was split across the initial year of the study to distribute the participant burden over time as noted in Supplemental Table 1. The health history survey was given at month 4, and the reproductive history was given at month 10. The Monthly Survey: Menstrual Update (MSMU) was initiated after the first completed month of enrollment and then monthly thereafter. The time to survey completion was estimated in 5-minute increments on the basis of usability testing by Apple, Inc. The response time for the enrollment processes (screening, eligibility, demographics) was estimated to be 25 minutes. The expected response times as listed in the Research app for monthly surveys such as the MSMU, Pregnancy Update, and Lactation Update were 5 minutes each.

Apple research app platform

The study is hosted within the Apple Research app (available on the Apple App Store), which allows a participant to find, enroll, and participate in Apple-supported, health-related research studies.

The Research app was designed with 3 studies for a simultaneous launch, where the demographics and certain questions were standardized across the studies. The other 2 studies were the Apple Heart and Movement Study and the Apple Hearing Study.[13,14]

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

All the shared data are stored securely in a system within Apple that is designed to meet the technical safeguard requirements of the Health Insurance Portability and Accountability Act. Access to any contact information or other identifying data that the participants provide through the Research app is restricted to the Principal Investigator staff.

Study population description

The AWHS is a longitudinal cohort study of persons who have menstruated at least once in their life. The study began enrolling on November 14, 2019. The planned duration of this study is 10 years, that is, until November 2029, with a potential for extension or additional long-term follow-up. The goal is to recruit 500,000 participants over 10 years. The study was approved by the Advarra Central Institutional Review Board (number PRO00037562) and registered to ClinicalTrials.gov (ClinicalTrials.gov Identifier: NCT04196595).

Eligibility, screening, and consent

Individuals were eligible for enrollment if they had installed the Apple Research app on their iPhone 6s or later with iOS version 13.2 or later, were living in the United States, had menstruated at least once, were at least 18 years old (at least 19 years old in Alabama and Nebraska, at least 21 years old in Puerto Rico), were comfortable communicating in written and spoken English, were the sole users of their iCloud account or iPhone, and were willing to provide informed consent to participate in the study (Supplemental Table 2).

After self-report and self-verification of eligibility, the participants followed the steps for enrollment as delivered by the Research app. They were instructed to read the informed consent form (ICF), which is included in Appendix A, and provide an electronic signature if they consented to participate; a part of this process is shown in Supplemental Figure 1. The ICF covers key aspects, including the study objectives, study procedures (surveys and demographic data), the types of study data that require additional consent (Health app Data, Research Sensor and Usage Data, Medical Conditions and History, and other related information such as clinically sourced data from Health app). The ICF included the participation risks (theoretical potential for breach of confidentiality) and benefits (no incentives or compensation) and the option for study withdrawal at any time for any reason. The current informed consent document is available in the supplemental documents. The participants who were enrolling were informed that they will be reconsented every 2 years.

The individuals who downloaded the Research app, enrolled in AWHS, and met the inclusion criteria proceeded to study participation. They were then provided the survey tasks for completion, starting with the demographics section.

Incentive: There was no compensation for study participation.

Recruitment and marketing

On September 10, 2019, the Apple Research app was announced publicly. The Research app houses the following 3 research studies: the AWHS, the Apple Heart and Movement Study, and the Apple Hearing Study. The AWHS was launched on November 14, 2019. Institutional review board-approved recruitment efforts included a Harvard T.H. Chan School of Public

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Health study website,[15] which was made public and includes frequently asked questions and background information regarding the study. Social media accounts were created on Twitter and Instagram (March 10, 2020), YouTube (March 12, 2020), Facebook (April 13, 2020) and LinkedIn (August 7, 2020) to post recruitment materials inviting potential participants to join the study, with new posts added approximately 1 to 3 times per week. In addition, media events included a podcast,[16] media articles, and press interviews after study launch.

Data Collection and Methods

Survey data

On enrollment, the participants who onboarded with the AWHS responded to the Research Profile Survey within the Research app and to the Demographic Survey; the data included the year of birth, state of residence, race and ethnicity, marital status, employment status, gender identity, and sex assigned at birth (Supplemental Figure 1 and Supplemental Table 3). The participants were asked to respond to a baseline Menstrual Status Survey at enrollment (Supplemental Table 3). The response categories for the baseline Menstrual Status Survey included currently menstruating, lactating, menopausal, and pregnant. For the remaining months within the first year of follow-up, the participants were given monthly surveys to provide a menstrual status update, pregnancy update, and/or a lactation update. Health surveys were given quarterly to assess the changes in sleep, physical activity, nutrition, stress, alcohol use, tobacco use, electronic nicotine use, and marijuana use within the previous calendar month. Reproductive history was assessed at the tenth month (Supplemental Table 1). As detailed in Supplemental Table 3, a more extensive health overview (including questions on nutrition, sleep, stress, alcohol use, tobacco use, electronic nicotine use, marijuana use, second-hand smoke, and overall self-rated health) and medical history (gynecologic, endocrine, heart, blood, digestive, kidney, lung, musculoskeletal, cancer, brain and nervous system, mental health and infectious disease conditions, surgeries, and family medical history) are given annually, initially at month 4 and month 7, respectively (Figure 1). A summary of the surveys, topics, sources, number questions is shown in Table 4.

Monthly surveys and timing

The participants receive monthly surveys on the basis of the status reported in the baseline Menstrual Status Survey. The monthly surveys include the MSMU, the Lactation Update, and the Pregnancy Update.

The MSMU included a total of 6 questions to ascertain the status in the last calendar month regarding the accuracy of tracked period days, status update for pregnancy, lactation, and menopause, current hormone use, reason for hormone use, and monthly update of health factors (change in exercise or weight, significant sleep disruption, stress, illness, and hospitalization or surgery). The purpose of the MSMU is to give additional context for the logged menstrual bleeding days and associated symptom logging in HealthKit. The MSMU is given to those who have previously indicated the capacity to currently menstruate on the baseline survey; it is not given to those who have indicated current pregnancy, menopause, or to those who are no longer menstruating. The MSMU is delivered within the Research

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

app on the first Sunday of every month, starting in month 2 of participation, at least 4 weeks after enrollment. The survey is available for 1 week after delivery and then expires and is no longer available to the participant. Programming logic was applied in the analysis phase as follows: the monthly surveys were counted when the participants responded at least 4 weeks after enrollment. Any monthly survey with participant responses before 4 weeks of enrollment was excluded from this count. For this analysis, the respondents were censored at pregnancy and menopause.

Research sensor and usage data

The participants consented to the collection of data and derived metrics that were retrieved from certain iPhone sensors and from a paired optional Apple Watch. These include frequently visited locations with an anonymized identifier, watch-on-wrist state, and Optical Sensor (including accelerometer and heart rate) as summarized in Supplemental Table 4.

HealthKit data

HealthKit provides a central repository for health and fitness data on iPhones and Apple Watches. With the user's permission, specific apps communicate with HealthKit to access and share these data while maintaining the user's privacy and control. HealthKit stores the data merged from multiple sources and contains data types such as menstrual bleeding days, symptoms and associated user recorded features (cervical mucous changes, temperature changes, sexual activity), heart rate, sleep analysis, and clinical records (lab tests, diagnoses) from clinical interfaces. A bleeding event can be tracked either via Cycle Tracking or by any third-party menstrual tracking application that has been permitted to write to HealthKit by the participant. This allows for ongoing collection of menstrual characteristics and symptoms and reduces missing data owing to lack of direct participant input. For this descriptive analysis, we evaluate the months of contributed cycle tracking data where a logged bleeding event in the HealthKit was attributed to the calendar month of that bleeding event.

Participation

This study was designed to allow participation through the following ways: (1) response to survey questions; (2) contribution of HealthKit data, which include logged menstrual cycles; and (3) contribution of SensorKit data, which include sensor-based data streams from SensorKit.

In general, a participant is considered to be actively participating by contributing data from any of these sources.

Given that one of the main goals of this study is to understand menstrual health and its risk factors, we report on

1. the response rates to the MSMU, and
2. tracked bleeding events in HealthKit as measures of ongoing participation for this descriptive analysis.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Nonparticipation in the MSMU is defined as no response to the monthly survey. Invalid responses are defined as those responses that seem biologically unlikely, such as a concurrent state of menopause and pregnancy. We defined completion rate (% completed) as the proportion of individuals who have completed the survey among those eligible for the baseline Menstrual Status Survey or MSMU.

Defining demographic variables

Race and ethnicity—We utilized the same question that was used to determine the race and ethnicity from the NIH-sponsored All of Us study, which asks, “Which categories describe you? Select all that apply: American Indian or Alaska Native [subchoices: American Indian, Alaska Native, Center or South American Indian, none of these fully describe me, I prefer not to answer]; Asian [subchoices: Asian Indian, Cambodian, Chinese, Filipino, Hmong, Japanese, Korean, Pakistani, Vietnamese, none of these fully describe me, I prefer not to answer]; Black, African American, or African [subchoices: African American, Barbadian, Caribbean, Ethiopian, Ghanaian, Haitian, Jamaican, Liberian, Nigerian, Somali, South African, none of these fully describe me, I prefer not to answer]; Hispanic, Latino, or Spanish [subchoices: Colombian, Cuban, Dominican, Ecuadorian, Honduran, Mexican or Mexican American, Puerto Rican, Salvadoran, Spanish, none of these fully describe me, I prefer not to answer]; Middle Eastern or North African [subchoices: Afghan, Algerian, Egyptian, Iranian, Iraqi, Israeli, Lebanese, Moroccan, Syrian, Tunisian, none of these fully describe me, I prefer not to answer]; Native Hawaiian or other Pacific Islander [subchoices: Chamorro, Chuukese, Fijian, Marshallese, Native Hawaiian, Palauan, Samoan, Tahitian, Tongan, none of these fully describe me, I prefer not to answer]; White [subchoices: Dutch, English, European (not listed), French, German, Irish, Italian, Norwegian, Polish, Scottish, Spanish, none of these fully describe me, I prefer not to answer]; none of these fully describe me; I prefer not to answer.” In field testing of the 2 questions typically used to separately determine the race and ethnicity, the All of Us study found that the focus group participants found it burdensome to have 2 questions. The All of Us study, where our race and ethnicity question is sourced from, uses a single question, with the response of “select all that apply” to determine the race and ethnicity. We have classified the responses into traditional reporting of race and ethnicity of the following categories: White, non-hispanic; Hispanic, Latina, Spanish and/or other Hispanic; Black or African American or African; Asian; Other; >1 race or ethnicity, in nonrestrictive categories.[17]

MacArthur social status scale and socioeconomic status—We utilized the MacArthur Scale of Subjective Social Status, which asks, “Think of this ladder as representing where people stand in the country you live in. At the top of the ladder are the people who are the best off – those who have the most money, the most education, and the most respected jobs. At the bottom are the people who are the worst off – those who have the least money, least education, the least respected jobs, or no job. The higher up you are on this ladder, the closer you are to the people at the very top; the lower you are, the closer you are to the people at the very bottom. Where would you place yourself on this ladder? Please select where you think you stand at this time in your life relative to other people around you. Ladder 0 (worst off) to 10 (best off).” The scale has been noted to correlate with health status across the lifespan.[18,19] Notably, the MacArthur Scale is correlated with but is

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

not the same as objective socioeconomic status (SES).[20] One main benefit of the MacArthur Scale is that it may be more applicable as a marker of subjective social status than using measures of objective SES in non-White populations.[18] We categorized the responses into: 0 to 3 corresponding to low, 4 to 5 corresponding to middle, and 6 to 9 corresponding to high. There are no established categorizations for this variable. We refer to this metric as the SES.

The study population described in this paper was enrolled from November 14, 2019 until May 20, 2020, and we allowed at least 6 months of follow-up for all the women enrolled during this time.

Planned statistical analyses—Statistical analyses are planned for the following 3 categories: (1) longitudinal analysis of survey data, (2) longitudinal analysis of passively collected smartphone and watch data, and (3) longitudinal analysis of associations between the survey data and passively collected data. In each category, we will perform exploratory descriptive analyses and formulate more specific hypothesis-driven models.

For all 3 types of longitudinal analyses, we will use longitudinal extensions of regression methods, such as linear and generalized linear mixed models,[21] statistical learning techniques for high-dimensional data,[22] and functional data analysis methods.[23] For the longitudinal analysis of the survey data, we will quantify the associations among both participant characteristics and risk factors and the menstrual cycle length, and how these associations vary across the age range of the study population. For the longitudinal analysis of passive data, we will perform individual-level analyses to identify the possible change points in behaviors over time and how they relate to subsequent health outcomes. For the longitudinal analysis of passive and survey data, the predictors will initially be the daily summary statistics derived from passively collected data and the outcomes of interest will consist of all the items on which survey data are available.

Study statistical power—We estimated the power to detect meaningful differences in (1) the mean menstrual cycle length and (2) the prevalence of health conditions of interest. We estimated loss to follow-up (20%) and incomplete survey response (90%–95%) over the course of 12 menstrual cycles. To calculate a conservative power estimate, we estimated a high incomplete survey response rate. This rate assumes an incomplete response if there is any skip of any question across the year. The survey is designed to not require a response to any question; a participant may choose not to answer by selecting a prefer not to answer response option or advancing through the survey questions. We present the conservative power calculations on the basis of a 2-sided alpha=0.01 test rather than the more common alpha=0.05 level (Supplemental Table 5).

Menstrual cycle—We estimated our power to detect the differences in the mean menstrual cycle length among a general dichotomy of the study sample. Such a comparison will be of interest when comparing the outcome across subpopulations defined by demographics (eg, race and ethnicity), lifestyle factors (eg, low or high physical activity), or potential exposures (eg, marijuana products or alcohol consumption) (Supplemental Table 6). Although the longitudinal methods will use all cycles from all participants, we evaluated scenarios where 5% to 10% of 400,000 participants provide menstrual cycle data on 12 cycles

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

and conservatively calculated minimally detectable differences in cycle length using data from those 5% to 10%. We assumed a two-sided alpha=0.01 test, and a within-participant longitudinal correlation in the cycle length of 0.6.[24] We estimate that we will have the power to detect the menstrual cycle length differences of <1 day for all the scenarios considered, as shown in Supplemental Table 6.

Gynecologic health conditions—We estimated the power of the study to detect differences in the prevalence of health conditions for high-risk vs low-risk groups for various initial sample sizes and health condition prevalence estimates in the baseline group (Supplemental Table 6). We estimate that we will have the power to detect relatively small differences in prevalence for all scenarios, even when the health condition is rare (0.5% prevalence), and the high-risk group is small (10% of the sample).

Results

Baseline characteristics of the first 10,000 participants

We present the demographic characteristics of the first 10,000 enrolled and eligible participants who provided demographic information and show their retention across the first 6 months of participation. From the launch of the study to May 20, 2020, there were 11,113 people who downloaded the Research app and clicked through to the AWHS, 10,459 who consented, and 10,030 who responded to the demographics survey. Eleven participants formally withdrew from the study within their first month of participation. The participant flow for the first 10,000 participants is shown in Figure 2. On average, 370 participants enrolled per week.

The mean (standard deviation) age at enrollment was 33.6 years (10.3). Although most of the participants were White and non-hispanic (69%), there were 12% Latina, 6% Black, 4% Asian, and 5% identifying as >1 race and ethnicity. Other races and ethnicities represented include American Indian or Alaskan Native (3%). Most participants had graduated college or beyond (51%), were employed for pay (either part-time, full-time, or self-employed) (70%), and reported the use of an Apple Watch (72%). Most participants also gender-identified as a ‘woman’ (96%) and were assigned ‘female’ at birth (99%). Forty percent of the participants were married and 33% were never married. The distribution of SES for the 10,000 participants on the MacArthur Scale are as follows: low (0–3): 31%, middle[4,5]: 42%, and high[6–9]: 25%. At the time of enrollment, more participants were living in the Southern region (35%) of the United States than any other but with many women also living in the Northeast (15%), Midwest (20%), and West (25%). A small proportion of women were living in the US territories (0.3%) or had no data available on their location (4%) (Table 1). The states with the most participants enrolled, adjusted for the total population by state from the 2010 census were Massachusetts, Alabama, and Oregon (Supplemental Figure 2). Menstrual tracking data in HealthKit (either retroactive data or data collected during study period) were available for 82.7% of the women, and SensorKit data on heart rate were available for 24% of the women (Table 1).

Supplemental Table 7 describes the selected characteristics obtained from ResearchKit of the 429 participants who enrolled in the study during the same time but did not respond

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

to the demographic questionnaire. Among these participants, the mean age was 34 years. When compared with enrollees that responded to the demographics questionnaire, a greater proportion of those who did not respond were from the South (40% vs 35%), fewer were Apple Watch users (45% vs 72%), and fewer opted-in to the authorization of SensorKit heart rate access (5% vs 24%).

On the basis of the self-reported menstrual status at the time of enrollment, 88% reported actively menstruating, 2% were lactating, 6% were menopausal, and 1% were pregnant. The baseline status and the monthly menstrual statuses across 6 months of follow-up are outlined in Table 2.

Retention

Among the first 10,000 enrollees, 6519 participated in at least 1 of the MSMU data collection (65.2%). Of those eligible, 3099 participants responded to the 6-month check-in (Table 1). 5748 participants responded to the first MSMU, and 4413 and 3902 responded to the second and third, respectively, as summarized in Table 3. The demographics of those at baseline (N=10,000) and those who responded to the month 6 questionnaire (N=3099) are shown in Table 1. The participants who contributed to the sixth MSMU were broadly similar to the enrolled cohort, differing mostly in being more likely to be educated, White, and unmarried. Among the consistent responders, more were Apple Watch users (83% vs 72%) and were associated with higher levels of tracking through HealthKit than the enrolled cohort.

Of the 10,000 participants enrolled, 82.7% tracked the menstrual bleeding days via HealthKit at some point in the 2-years before study entry or in the 6 months of follow-up. 72.4% of the participants tracked at least 1 menstrual bleeding event during the 6-month follow-up period, and the participants tracked an average of 4.44 (25%–75%; range, 3–6) calendar months during the study period. Among those who completed the sixth MSMU, 95.1% contributed a tracked bleeding event, and 91.4% tracked at least 1 menstrual bleeding event during the 6-months of follow-up. Among this subset, the participants tracked an average of 5.29 (25%–75%; range, 5–6) months of cycle data (Table 1).

Survey response time

The participants spent a median time of 1.83 minutes to complete the demographic survey (25th–75th percentile range, 1.43–2.45 minutes) and a median time of 0.77 minutes to complete the MSMU (25th–75th percentile range, 0.55–1.10 minutes) and are noted in Supplemental Table 10.

Discussion

Principal findings

This is the first app-based study of this scope with the goal of collecting longitudinal data for at least 10 years. Among the first 10,000 participants enrolled, the principle findings of this study are that (1) the racial and ethnic distribution of the enrolled cohort was similar to that of the US population, (2) Non-White participants were slightly more likely to drop

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

out of the study than White participants over 6 months of follow-up, (3) the participant geographic distribution of the AWHS included all the US states and Puerto Rico, (4) most of the participants had graduated college or beyond, were employed for pay, and reported the use of an Apple Watch.

Clinical implications

The study aims to advance the understanding of menstrual cycles, the factors affecting both within-woman and between-woman variability, and the associations with various health conditions. The study will have novel opportunities to examine variations in reproductive physiology using passively collected data such as physical activity and heart rate. The possible clinical implications include understanding the associations between population-based exposures among iPhone users and the reproductive outcomes including the menstrual cycle length and irregularity, infertility, menopause, and chronic diseases such as cancer and heart disease measured via Health Records in HealthKit.

Research implications

Among the 10,502 participants who downloaded the app and were eligible, 96% enrolled and responded to the demographics section, which compares favorably with other longitudinal studies.[25–27] The recruitment efforts were generally not targeted to specific populations but mainly comprised general media coverage and social media posts. Thirty-eight percent of the participants did not respond to the MSMU after enrollment, with a total of 35% of participants responding to the MSMU at the 6-month follow-up. At least 1 menstrual cycle was tracked via HealthKit, by 82.7% (8266/10,000) of the initial cohort and 95.1% (2948/3,099) of the participants who responded to month 6 of the MSMU. The participants contributed with an average of 4.44 (25%–75%; range, 3–6) tracked calendar months during the 6-month follow-up period. Although the race and ethnicity distribution at the baseline was more closely representative of the US population, we noted a slight increase in the proportion of White (Non-Hispanic) race and ethnicity and a higher education status for the participants responding to month 6 of the MSMU than the participants at enrollment. It is to be noted that the survey completion times were considerably shorter than expected.

Strengths and limitations

The AWHS overcomes several limitations of the existing studies of menstrual cycle characteristics including the following: (1) not restricting to those women attempting conception,[25,28] (2) low responses to reproductive questions surrounding menstrual cycle characteristics,[26] (3) underascertainment of the menstrual cycle characteristics for cycle-specific analysis.[9] Furthermore, many existing cohorts lack ascertainment on basic reproductive history and menstrual cycle characteristics, despite having well-characterized outcome data for the leading causes of mortality and morbidity.[29] This study builds on the Tremin study[7] by extending racial and ethnic diversity and obtaining expanded demographic, anthropometric, lifestyle, and behavioral data elements from HealthKit and Research Sensor and Usage Data, which allow for unique exposure and outcomes assessment. Furthermore, though the findings may have limited generalizability outside of iPhone users, the digital platform may increase access, allowing participants to engage with this digital study.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Although the study has many strengths, several limitations must be considered. Firstly, the study is limited to Apple iPhone users, and there is a concern of generalizability to other populations using other digital platforms. Secondly, the loss to follow-up measured by the response rates for the Monthly Survey: Menstrual Updates (MSMU) is higher than other retention metrics such as tracked menstrual bleeding events in HealthKit. We have initiated the retention efforts utilizing education, communication, and engagement through a study update feature within the app and on the study website to promote monthly survey completion. To ensure continued diversity in this cohort, care must be taken to both recruit and retain the population through effective engagement strategies. Furthermore, engagement strategies may be constructed to limit the loss to follow-up of certain subpopulations. Further evaluation of the data must be conducted to understand whether nonrandom dropout may bias the longitudinal effect estimates on the basis of the monthly surveys, though the menstrual data that is tracked will be written to HealthKit, and it will limit missingness and avoid reliance on survey responses.

Conclusion

The AWHS captures time-varying demographic, lifestyle, and behavioral data that are built into the Research app, an app that interfaces with multiple data sources. These data streams create an opportunity for the AWHS to contribute new knowledge about long-overlooked and understudied women's health issues.

Supplementary Material

Refer to Web version on PubMed Central for supplementary material.

Acknowledgments

The AWHS team would like to thank all the participants for signing up for the study and contributing to the advancement of women's health research. We would like to acknowledge Kaitlyn Haughey, MS, Manasvi Marathe, MPH, and Jill MacRae, MS, for their work in supporting the study as a part of the Harvard Study Staff at study initiation; Michael Grusby, PhD, who was involved in the initial phase of this project; the Harvard Information Technology Team, including Andy Ross, BCS, Noah Hulbert, MBA; and David Waxman, MBA, from the Office of Financial Services. We would like to acknowledge Richa Gujarati, MBA, former marketing team lead at Apple, Inc, for supporting the recruitment efforts for this project.

S.M. receives research funding from the National Institutes of Health (NIH), National Science Foundation, and March of Dimes. R.H. receives research funding from the NIH. B.A.C. receives research funding from the NIH and the United States Environmental Protection Agency. J.P.O. receives research funding from the NIH, Boehringer Ingelheim. J.P.O. received an unrestricted gift from Mindstrong Health in 2018. J.P.O. is a cofounder of a recently established commercial entity that operates in digital phenotyping outside of women's health. C.L.C., T.F.C., G.A. own Apple, Inc stock. The other authors report no conflict of interest.

This study received funding from Apple, Inc. The funder had no role in the analysis and interpretation of data. Support for A.M.Z.J., K.K.F., D.D.B., and A.J.W. was provided by the Intramural Research Program of the National Institute of Environmental Health Sciences, National Institutes of Health.

References

1. Wang YX, Arvizu M, Rich-Edwards JW, et al. Menstrual cycle regularity and length across the reproductive lifespan and risk of premature mortality: prospective cohort study. BMJ 2020;371:m3464. [PubMed: 32998909]

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

2. Seifert-Klauss V, Prior JC. Progesterone and bone: actions promoting bone health in women. J Osteoporos 2010;2010:845180. [PubMed: 21052538]
3. Wesselink AK, Wise LA, Hatch EE, et al. Menstrual cycle characteristics and fecundability in a North American preconception cohort. Ann Epidemiol 2016;26:482–7.e1. [PubMed: 27449569]
4. Arendt LM, Kuperwasser C. Form and function: how estrogen and progesterone regulate the mammary epithelial hierarchy. J Mammary Gland Biol Neoplasia 2015;20:9–25. [PubMed: 26188694]
5. Sundström Poromaa I, Gingnell M. Menstrual cycle influence on cognitive function and emotion processing-from a reproductive perspective. Front Neurosci 2014;8:380. [PubMed: 25505380]
6. Liu Z, Doan QV, Blumenthal P, Dubois RW. A systematic review evaluating health-related quality of life, work impairment, and health-care costs and utilization in abnormal uterine bleeding. Value Health 2007;10:183–94. [PubMed: 17532811]
7. Treloar AE, Boynton RE, Behn BG, Brown BW. Variation of the human menstrual cycle through reproductive life. Int J Fertil 1967;12:77–126. [PubMed: 5419031]
8. Bull JR, Rowland SP, Scherwitzl EB, Scherwitzl R, Danielsson KG, Harper J. Real-world menstrual cycle characteristics of more than 600,000 menstrual cycles. NPJ Digit Med 2019;2:83. [PubMed: 31482137]
9. Bao Y, Bertoia ML, Lenart EB, et al. Origin, methods, and evolution of the three nurses' health studies. Am J Public Health 2016;106:1573–81. [PubMed: 27459450]
10. Harvard University. The ovulation and menstruation health (OM) pilot study survey instrument. 2020. Available at: https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/XACYQA. Accessed December 14, 2020.
11. All of Us Research Program Investigators, Denny JC, Rutter JL, et al. The "All of Us" Research Program. N Engl J Med 2019;381:668–76. [PubMed: 31412182]
12. Cohen S, Kamarck T, Mermelstein R. A global measure of perceived stress. J Health Soc Behav 1983;24:385–96. [PubMed: 6668417]
13. Brigham and Women's Hospital. Apple heart and movement study. Available at: http://www.bwhresearch.org/appleheartandmovementstudy/. Accessed December 16, 2020.
14. University of Michigan. Michigan public health apple hearing study. 2021. Available at: https://sph.umich.edu/applehearingstudy/. Accessed December 16, 2020.
15. Harvard TH. Chan School of Public Health. Apple women's health study. 2019. Available at: https://www.hsph.harvard.edu/applewomenshealthstudy/. Accessed December 16, 2020.
16. Mahalingaiah S, Onnela J, Levin D. Gaining insight into women's health. 2020. Available at: https://harvard-chan-this-week-in-health.simplecast.com/episodes/womens-health. Accessed December 18, 2020.
17. Coughlin SS, Chen J, Cortes JE. Health care access and utilization among adult cancer survivors: results from the National Institutes of Health "All of Us" Research Program. Cancer Med 2021;10:3646–54. [PubMed: 33942535]
18. Adler N, Singh-Manoux A, Schwartz J, Stewart J, Matthews K, Marmot MG. Social status and health: a comparison of British civil servants in Whitehall-II with European- and African-Americans in CARDIA. Soc Sci Med 2008;66:1034–45. [PubMed: 18180089]
19. Stanford University. MacArthur Scale of Subjective Social Status – Adult Version. 2018. Available at: https://sparqtools.org/mobility-measure/macarthur-scale-of-subjective-social-status-adult-version/. Accessed October 18, 2021.
20. Tan JJX, Kraus MW, Carpenter NC, Adler NE. The association between objective and subjective socioeconomic status and subjective well-being: a meta-analytic review. Psychol Bull 2020;146:970–1020. [PubMed: 33090862]
21. Fitzmaurice GM, Laird NM, Ware JH. Applied longitudinal analysis, 2nd ed. New York, NY: Wiley; 2011.
22. Hastie T, Silverman B. The elements of statistical learning, 2nd ed. New York, NY: Springer; 2009.
23. Ramsay J, Silverman B. Functional data analysis, 2nd ed. New York, NY: Springer; 2005.
24. Lisabeth L, Harlow SD, Lin X, Gillespie B, Sowers M. Sampling strategies for prospective studies of menstrual function. Am J Epidemiol 2004;159:795–802. [PubMed: 15051589]

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

25. Wise LA, Rothman KJ, Mikkelsen EM, et al. Design and conduct of an internet-based preconception cohort study in north America: pregnancy study online. Paediatr Perinat Epidemiol 2015;29:360–71. [PubMed: 26111445]
26. McManus DD, Trinquart L, Benjamin EJ, et al. Design and preliminary findings from a new electronic cohort embedded in the Framingham Heart Study. J Med Internet Res 2019;21:e12143. [PubMed: 30821691]
27. Mahalingaiah S, Cosenza C, Cheng JJ, Rodriguez E, Aschengrau A. Creating a survey instrument for self-assessed menstrual cycle characteristics and androgen excess. 2020. Available at: https://www.medrxiv.org/content/10.1101/2020.03.03.20030676v1.full. Accessed December 14, 2020.
28. Buck Louis GM, Schisterman EF, Sweeney AM, et al. Designing prospective cohort studies for assessing reproductive and developmental toxicity during sensitive windows of human reproduction and development–the LIFE Study. Paediatr Perinat Epidemiol 2011;25:413–24. [PubMed: 21819423]
29. Pino EC, Zuo Y, Maciel De Olivera C, et al. Cohort profile: the MULTI sTUdy Diabetes rEsearch (MULTITUDE) consortium. BMJ Open 2018;8:e020640.
30. Centers for Disease Control and Prevention (CDC). Behavioral Risk Factor Surveillance System. 2019. Available at: https://www.cdc.gov/brfss/questionnaires/index.htm. Accessed August 15, 2021.
31. Chew LD, Bradley KA, Boyko EJ. Brief questions to identify patients with inadequate health literacy. Fam Med 2004;36:588–94. [PubMed: 15343421]
32. Centers for Disease Control and Prevention. NHANES 2017-2018 Questionnaire Instruments. Available at: https://wwwn.cdc.gov/nchs/nhanes/continuousnhanes/questionnaires.aspx?BeginYear=2017. Accessed August 15, 2021.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

AJOG at a Glance

Why was this study conducted?

The Apple Women's Health Study aims to advance the understanding of menstrual cycles and their relationship to health conditions such as infertility, menopause, and health across the lifespan. This paper describes the study design and methods, the demographics of the first 10,000 enrollees, and the study retention rates measured by the response to the Monthly Survey: Menstrual Update and menstrual tracking in HealthKit.

Key findings

The racial and ethnic distribution of the enrolled cohort was similar to that of the US population. Non-White participants were slightly more likely to drop out of the study than White participants over 6 months of follow-up. Notably, 38% (3490/9238 eligible participants) of the cohort did not respond to the Monthly Survey: Menstrual Update after enrollment. Thirty-five percent (3099/8972) of women who were eligible responded to the 6-month Monthly Survey: Menstrual Update. The participants tracked their menstrual bleeding days for an average of 4.44 (25%–75%; range, 3–6) calendar months during the 6 month follow-up period. In addition, 82.7% (8266/10,000) of the cohort tracked at least one menstrual cycle via HealthKit.

What does this add to what is known?

This is the first longitudinal research study of this scale and scope to use a mobile application to collect survey and sensor-based data on menstrual cycles and women's health.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Participant Data Collection	At enrollment	Within first year	Annually	Quarterly	Monthly	Daily	Every 2 years	Qualifying IRB amendment
Informed Consent	●						●	●
Request for Passive Data Collection	●						●	
Passive Data Collection						●		
Research Profile - Demographics	●		●					
Menstrual Status Survey	●							
Monthly Survey					●			
Quarterly Health Survey				●				
Annual Health Survey		●	●					
Annual Medical History		●	●					
Reproductive History		●						

FIGURE 1.
Timeline of data collection

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

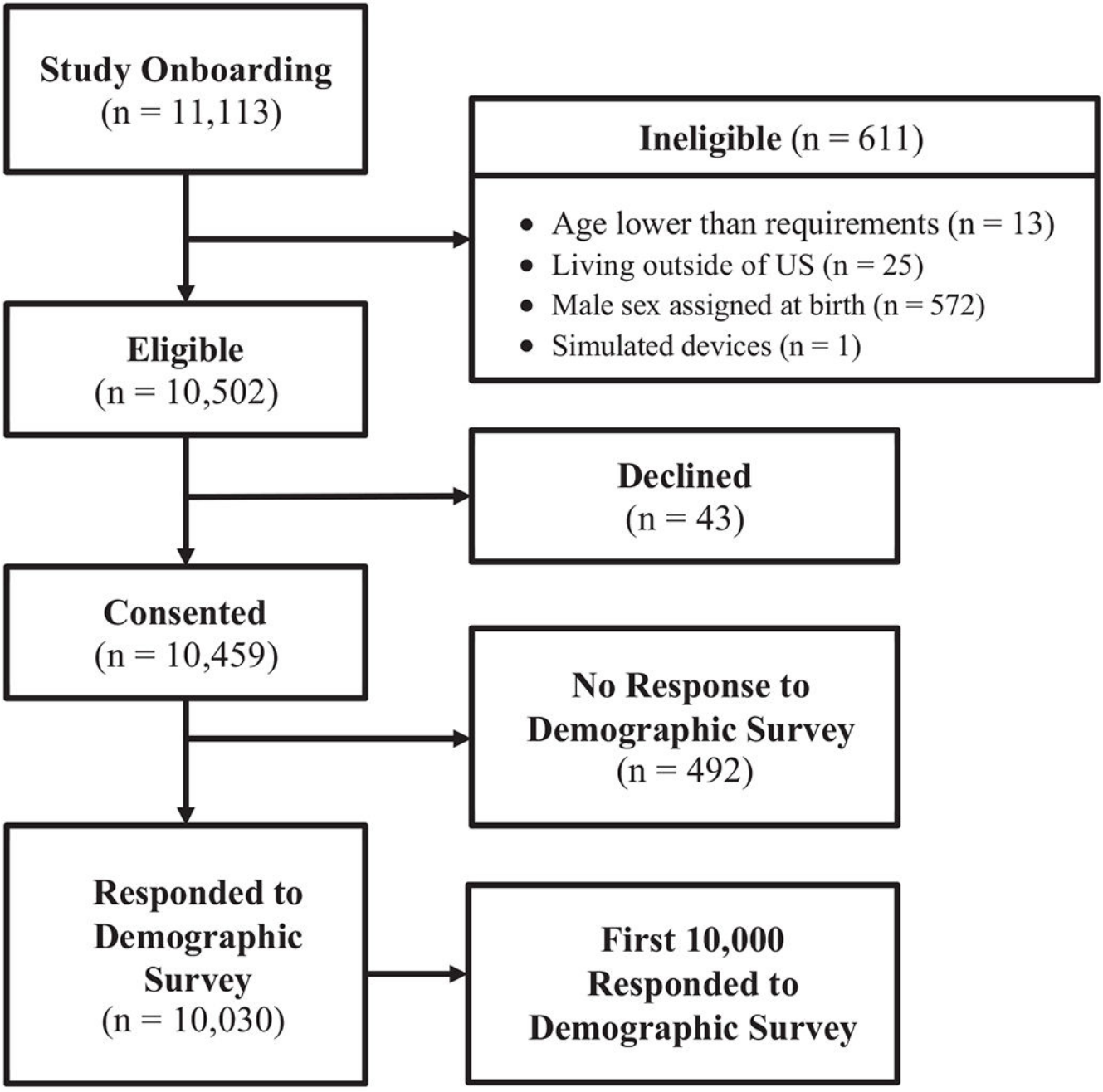


FIGURE 2.

Participant flow in the Apple Women's Health Study, first 10,000 participants. Study onboarding as of May 20, 2020; categories of ineligibility are not mutually exclusive

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 58 of 217

TABLE 1

Demographics of Apple Women's Health Study participants

Demographics	Participants at baseline, first 10,000 participants[a] Mean±SD or mean (25%–75% range) or % (n)	Participants responding to month 6 of the "Monthly Survey: Menstrual Update" (n=3099)[a] Mean±SD or mean (25%–75% range) or % (n)
Age (y),[b] mean±SD	33.6±10.3	33.0±8.5
Race, % (n)		
White, non-Hispanic	69.1 (6910)	73.7 (2284)
Hispanic, Latina, Spanish and/or other Hispanic[c]	12.0 (1202)	10.2 (317)
Black or African American or African	6.1 (609)	4.7 (147)
Asian	4.3 (428)	4.4 (135)
Other	2.7 (274)	2.2 (67)
>1 race	5.1 (513)	4.7 (145)
Prefer not to answer, or missing	0.6 (64)	0.1 (4)
Gender identity, % (n)		
Woman	96.1 (9612)	97.2 (3013)
Man	0.3 (31)	<0.1 (3)
Transwoman	<0.1 (1)	0 (0)
Transman	0.17 (17)	<0.1 (3)
Genderqueer or nonbinary	1.04 (104)	1.3 (39)
Another gender identity or multiple selected	0.9 (92)	0.8 (25)
I prefer not to answer	0 (0)	0 (0)
Skip or missing	1.4 (143)	0.5 (16)
Sex assigned at birth, % (n)		
Female	98.5 (9845)	99.5 (3085)
Intersex	0.2 (19)	0 (0)
Skip or missing	1.3 (136)	0.5 (14)
Education, n (%)		
Never attended school or only attended kindergarten	0.2 (18)	<0.1 (1)

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Demographics	Participants at baseline, first 10,000 participants[a] Mean±SD or mean (25%–75% range) or % (n)	Participants responding to month 6 of the "Monthly Survey: Menstrual Update" (n=3099)[a] Mean±SD or mean (25%–75% range) or % (n)
Grades 1 through 11 (primary, middle, or some high school)	2.5 (250)	1.3 (39)
Grade 12 or GED (high school graduate)	12.4 (1237)	9.1 (280)
1 to 3 y after high school (technical school or some college or associate's degree)	32.6 (3261)	29.1 (904)
College 4 y or more (college graduate)	30.5 (3053)	35.5 (1099)
Master's degree	15.6 (1563)	18.9 (586)
Doctorate degree	4.7 (473)	5.5 (171)
I prefer not to answer	0 (0)	0 (0)
Skip or missing	1.5 (145)	0.6 (19)
Employment status, % (n)		
Employed for pay (part-time, full-time, self-employed)	70.3 (7031)	77.1 (2388)
Unemployed	5.6 (559)	3.5 (109)
Unable to work (ie, disability, illness, other circumstances)	4.2 (417)	2.8 (86)
In school	11 (1102)	10.7 (331)
Taking care of house or family	5.9 (584)	5.0 (156)
In retirement	1.5 (152)	0.2 (7)
I prefer not to answer	0.9 (97)	0.5 (14)
Missing	0.6 (58)	0.3 (8)
Marital status, % (n)		
Married	39.6 (3951)	41.5 (1285)
Divorced	8.3 (831)	6.8 (210)
Widowed	0.8 (82)	0.4 (12)
Separated	1.9 (194)	1.4 (43)
Never married	33.5 (3347)	34.6 (1071)
A member of an unmarried couple	14.2 (1416)	14.5 (450)
I prefer not to answer	0 (0)	0 (0)
Skip or missing	1.8 (179)	0.9 (28)
Socioeconomic status, % (n)		

Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 59 of 217

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Demographics	Participants at baseline, first 10,000 participants[a] Mean±SD or mean (25%–75% range) or % (n)	Participants responding to month 6 of the "Monthly Survey: Menstrual Update" (n=3099)[a] Mean±SD or mean (25%–75% range) or % (n)
0–3	31.5 (3146)	33.3 (1032)
4–5	42.2 (4223)	44.4 (1376)
6–9	25.4 (2535)	21.9 (678)
Missing	0.96 (96)	0.4 (13)
Region of the United States, % (n)		
Northeast	15.3 (1528)	15.6 (484)
Midwest	20.3 (2033)	20.9 (649)
South	34.8 (3477)	32.7 (1013)
West	24.9 (2492)	25.8 (801)
Territory	0.3 (25)	0.3 (8)
Data not available	4.5 (445)	4.6 (144)
Apple Watch users, % (n)	72.2 (7223)	82.5 (2557)
Heart Rate SensorKit Data Opt-In Authorization, % (n)	24.4 (2438)	31.2 (968)
Menstrual flow HealthKit tracking		
Tracked at least 1 menstrual cycle ever, % (n)	82.7 (8266)	95.1 (2948)
Tracked at least 1 menstrual cycle within 3 mo of enrollment, % (n)	70.6 (7064)	89.5 (2772)
Tracked at least 1 menstrual cycle within 6 mo of enrollment, % (n)	72.4 (7236)	91.4 (2833)
Average number of calendar months tracked before baseline	8.08 (25%–75%; range, 2–13)	9.12 (25%–75%; range, 3–16)
Average number of calendar months tracked within 3 mo of enrollment (among those tracking)[d]	2.67 (25%–75%; range, 2–3)	2.94 (25%–75%; range, 3–4)
Average number of calendar months tracked within 6 mo of enrollment (among those tracking)[d]	4.44 (25%–75%; range, 3–6)	5.29 (25%–75%; range, 5–6)

GED, general equivalency diploma; *SD*, standard deviation.

[a]Subset for the first 10,000 participants enrolled and providing demographic data that met inclusion criteria (through May 20, 2020). First demographics entry captured for each participant;

[b]Age based on birth year;

[c]Includes all individuals identifying as Hispanic (exclusively or in addition to another race group). Detailed breakdown available in Supplemental Table 8;

[d]Number of calendar months where any bleeding events were tracked during the 3 month follow-up period can range in value from 0 to 4 because a single menstrual cycle can span 2 calendar months. Number of calendar months tracked during the 6 month follow-up period can range from 0 to 7 months.

Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 60 of 217

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 61 of 217

TABLE 2

Monthly menstrual survey status count

Menstrual status	Baseline % (n)	Survey #1 % (n)	Survey #2 % (n)	Survey #3 % (n)	Survey #4 % (n)	Survey #5 % (n)	Survey #6 % (n)
Menstruating	87.6 (8763)	55.4 (5540)	42.7 (4274)	37.9 (3791)	36.6 (3659)	33.6 (3355)	30.2 (3021)
Lactation	1.8 (183)	1.0 (102)	0.8 (83)	0.6 (61)	0.5 (53)	0.5 (45)	0.4 (38)
Menopause	6.3 (634)	0.3 (26)	0.2 (22)	0.1 (11)	<0.1 (6)	0.1 (10)	<0.1 (5)
Pregnant	1.1 (110)	0.7 (67)	0.3 (32)	0.4 (35)	0.3 (31)	0.3 (26)	0.3 (32)
Invalid response[a]	<0.1 (7)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Prefer not to answer	0.5 (54)	0.1 (13)	<0.1 (2)	<0.1 (4)	<0.1 (2)	<0.1 (1)	<0.1 (2)
No response[b]	2.5 (249)	34.9 (3490)	47.3 (4732)	51.9 (5189)	52.9 (5293)	55.7 (5571)	58.7 (5873)
Ineligible[c]	-	7.6 (762)	8.6 (855)	9.1 (909)	9.6 (955)	9.9 (992)	10.3 (1028)

Subset for the first 10,000 participants enrolled and providing demographic data that met inclusion criteria (through May 20, 2020).

[a]Invalid Responses include those that are not biologically feasible (eg, “Pregnant” & “Menopause”) and are most likely because of user error;

[b]There is no metadata captured for individuals who do not respond to the baseline or monthly surveys. This value is derived from subtracting the “Count Completed” column from the “Count Eligible” columns in Table 2;

[c]Individuals who reported a menstrual status of “Menopause,” “Pregnant,” or with an invalid response at baseline or in the monthly survey during a prior month are not eligible to receive the survey in subsequent months. In addition, participants who withdrew (N=11) from the study are not eligible to receive the survey. The ‘Ineligible’ group is a cumulative sum across the 6 month follow-up period.

Am J Obstet Gynecol. Author manuscript; available in PMC 2023 September 25.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 62 of 217

TABLE 3

Monthly menstrual survey response totals

Menstrual survey number	Count completed	Count eligible[a]	Percentage completed[b]
Baseline	9751	10,000	97.5
1	5748	9238	62.2
2	4413	9145	48.3
3	3902	9091	42.9
4	3752	9045	41.5
5	3437	9008	38.2
6	3099	8972	34.5

[a]Subset for the first 10,000 participants enrolled and providing demographic data that met inclusion criteria (through May 20, 2020). Monthly menstrual surveys started in January 2020. Consecutive responses to surveys not required. Individuals who reported a menstrual status of “Menopause” or “Pregnant” at baseline or in the monthly survey were not eligible to receive the survey in subsequent months. In addition, participants who withdrew from the study (N=11) are not eligible to receive the survey;

[b]Percentage completed refers to proportion of individuals who were eligible to receive the baseline or monthly menstrual survey and completed the survey. Calculated using the ‘Count Completed’ and ‘Count Eligible’ columns.

Author Manuscript Author Manuscript Author Manuscript Author Manuscript

Case 3:23-cv-04597-EMC Document 307-1 Filed 03/13/26 Page 63 of 217

TABLE 4

Summary of surveys, topics, number and source of questions

Surveys		Topics	Number of questions	Source of questions
Profile		Name, date of birth, email, phone number, country, and state.	7	Study-specific
Demographics		Race and ethnicity, social economic status, zip code, body measurements, sex, gender identity	11	Study-specific, All of Us study (NIH), Behavioral Risk Factor Surveillance System, Centers for Disease Control and Prevention, US Census Current Population Survey, MacArthur Scale of Subjective Social Status
Menstrual status survey		Menstrual status, tracking cycles, tracking pregnancy, tracking health	4	Study-specific
Monthly survey	Menstrual update	Menstrual status, monthly tracking check-in, hormone use, health factors, pregnancy planning	6	Study-specific
	Pregnancy update	Pregnancy update, due date, pregnancy details, lactation.	10	Study-specific
	Lactation update	Lactation update	1	Study-specific
Annual health survey		Physical activity, nutrition, sleep habits, stress level, alcohol use, tobacco use, electronic nicotine use, marijuana use, second-hand smoke, overall health	30	Study-specific, National Health and Nutrition Examination Survey, Centers for Disease Control and Prevention, Perceived Stress Scale, All of Us study (NIH)
Quarterly health survey		Health update (sleep, nutrition, physical activity, stress, alcohol use, nicotine use)	6	Study-specific
Annual medical history		Menstrual status; gynecologic, endocrine, heart, blood, digestive, kidney, lung, musculoskeletal, mental health and brain and nervous system conditions; cancer, infectious diseases, surgeries, gynecologic surgeries, gender and sexual orientation, family medical history, medical forms	24	Study-specific, Derived from OM Study, and Brief Health Literacy Screening Tool
Reproductive history		Participant's birth details, early menstrual cycles, hormone use, hormone use details, pregnancy history	18	Study-specific and Derived from OM Study

Adapted from Harvard University,[10] Denny et al,[11] Cohen et al,[12] Adler et al,[19] Centers for Disease Control and Prevention,[30] Chew et al,[31] Centers for Disease Control and Prevention.[32]

NIH, National Institutes of Health.

J. EXHIBIT J: CLINICALTRIALS.GOV

Exhibit **ClinicalTrials.gov** registration for Apple's study, identifier NCT04196595,

Glossary

Glossary

ClinicalTrials.gov

National Library of Medicine
National Center for Biotechnology Information

Record 8 of 26

The U.S. government does not review or approve the safety and science of all studies listed on this website.

Read our full disclaimer (https://clinicaltrials.gov/about-site/disclaimer) for details.

Recruiting

Apple Women's Health Study

ClinicalTrials.gov ID NCT04196595

Sponsor Apple Inc.

Information provided by Apple Inc. (Responsible Party)

Last Update Posted 2024-07-03

Study Details Tab

Study Overview

Brief Summary

This is an observational longitudinal study to advance the understanding of menstrual cycle and gynecologic health conditions including PCOS, infertility and breast cancer.The study will be hosted within the Research app(available on App Store), which allows a user to find, enroll, and participate in Apple-supported health-related research studies.

Official Title

Apple Women's Health Study

Conditions

Menstrual Cycle | Ovulation | Menstruation | Polycystic Ovary Syndrome | Infertility | Menopause | Reproduction | Reproductive Health

Other Study ID Numbers

- Pro00037562

Study Start (Actual)

2019-11-14

Primary Completion (Estimated)

2029-11

Study Completion (Estimated)

2029-11

Enrollment (Estimated)

500000

Study Type

Observational

Resource links provided by the National Library of Medicine

MedlinePlus Genetics (https://medlineplus.gov/genetics/) related topics: Polycystic ovary syndrome (https://medlineplus.gov/genetics/condition/polycystic-ovary-syndrome)

MedlinePlus (https://medlineplus.gov/) related topics: Infertility (https://medlineplus.gov/infertility.html) Polycystic Ovary Syndrome (https://medlineplus.gov/polycysticovarysyndrome.html)

FDA Drug and Device Resources (https://clinicaltrials.gov/fda-links)

Contacts and Locations

This section provides contact details for people who can answer questions about joining this study, and information on where this study is taking place.

To learn more, please see the Contacts and Locations section in How to Read a Study Record (https://clinicaltrials.gov/study-basics/how-to-read-study-record#contacts-and-locations).

Study Contact

Name: Shruthi Mahalingaiah, MD
Phone Number: 617-432-1356
Email: AppleWomensHealthStudy@hsph.harvard.edu

This study has 1 location

United States

Massachusetts Locations

Boston, Massachusetts, United States, 02115
Recruiting
Harvard T.H. Chan School of Public Health
Contact : Shruthi Mahalingaiah
617-432-1356
AppleWomensHealthStudy@hsph.harvard.edu

Participation Criteria

Researchers look for people who fit a certain description, called eligibility criteria. Some examples of these criteria are a person's general health condition or prior treatments.

For general information about clinical research, read Learn About Studies (https://clinicaltrials.gov/study-basics/learn-about-studies).

Eligibility Criteria

Description

Inclusion Criteria:

- Have menstruated at least once
- Be at least 18 years old (at least 19 years old in Alabama and Nebraska, at least 21 years old in Puerto Rico)
- Live in the United States of America
- Be comfortable communicating in written and spoken English
- Have installed the Apple Research app on your iPhone
- Not share your iCloud account or iPhone with anyone else
- Be willing and able to provide informed consent to participate in the study

Study Population

Convenience sampling of individuals who have ever menstruated and meet other eligibility criteria

Ages Eligible for Study

18 Years and older (Adult, Older Adult)

Sexes Eligible for Study

All

Accepts Healthy Volunteers

Yes

Sampling Method

Non-Probability Sample

Study Plan

This section provides details of the study plan, including how the study is designed and what the study is measuring.

How is the study designed?

Design Details

Observational Model : Cohort
Time Perspective: Prospective

What is the study measuring?

Primary Outcome Measures

Outcome Measure	Measure Description	Time Frame
Identify Menstrual Cycle Patterns	Characterized using duration of menstrual flow, and cycle length in unit of days.	Up to 10 years
Epidemiologic Description of Menstrual Cycle	Characterized using cycle patterns and self-reported demographics, no unit of measure	Up to 10 years

Secondary Outcome Measures

Outcome Measure	Measure Description	Time Frame
Determine prevalence of gynecologic health conditions	Characterized using menstrual cycle patterns and self-reported health conditions, no unit of measure	Up to 10 years

Collaborators and Investigators

This is where you will find people and organizations involved with this study.

Sponsor

Apple Inc.

Collaborators

- Harvard School of Public Health (HSPH)
- National Institute of Environmental Health Sciences (NIEHS)

Investigators

- Principal Investigator: Michelle A Williams, SM, ScD, Harvard School of Public Health (HSPH)
- Principal Investigator: Russ B Hauser, MD, MPH, ScD, Harvard School of Public Health (HSPH)
- Principal Investigator: Brent A Coull, PhD, Harvard School of Public Health (HSPH)
- Principal Investigator: Shruthi Mahalingaiah, MD, MS, Harvard School of Public Health (HSPH)

Publications

From PubMed

These publications are automatically filled in from PubMed, a public database of scientific and medical articles, and may or may not be about the study.

- Zhang CY, Li H, Zhang S, Suharwardy S, Chaturvedi U, Fischer-Colbrie T, Maratta LA, Onnela JP, Coull BA, Hauser R, Williams MA, Baird DD, Jukic AMZ, Mahalingaiah S, Curry CL. Abnormal uterine bleeding patterns determined through menstrual tracking among participants in the Apple Women's Health Study. Am J Obstet Gynecol. 2023 Feb;228(2):213.e1-213.e22. doi: 10.1016/j.ajog.2022.10.029. Epub 2022 Oct 29. (https://pubmed.ncbi.nlm.nih.gov/36414993)

Study Record Dates

These dates track the progress of study record and summary results submissions to ClinicalTrials.gov. Study records and reported results are reviewed by the National Library of Medicine (NLM) to make sure they meet specific quality control standards before being posted on the public website.

Study Registration Dates

First Submitted

2019-11-13

First Submitted that Met QC Criteria

2019-12-10

First Posted

2019-12-12

Study Record Updates

Last Update Submitted that Met QC Criteria

2024-07-01

Last Update Posted

2024-07-03

Last Verified

2024-07

More Information

Terms related to this study

Keywords Provided by Apple Inc.

Menstruation
Menstrual Cycle
Ovulation
Polycystic Ovary Syndrome
Infertility
Menopause
Reproduction
Reproductive Health

Additional Relevant MeSH Terms

Ovarian Cysts
Cysts
Neoplasms
Ovarian Diseases

Adnexal Diseases
Genital Diseases, Female
Female Urogenital Diseases
Female Urogenital Diseases and Pregnancy Complications
Urogenital Diseases
Genital Diseases
Gonadal Disorders
Endocrine System Diseases
Polycystic Ovary Syndrome
Infertility

Plan for Individual Participant Data (IPD)

Plan to Share Individual Participant Data (IPD)?

Undecided

Drug and device information, study documents, and helpful links

Studies a U.S. FDA-Regulated Drug Product

No

Studies a U.S. FDA-Regulated Device Product

No

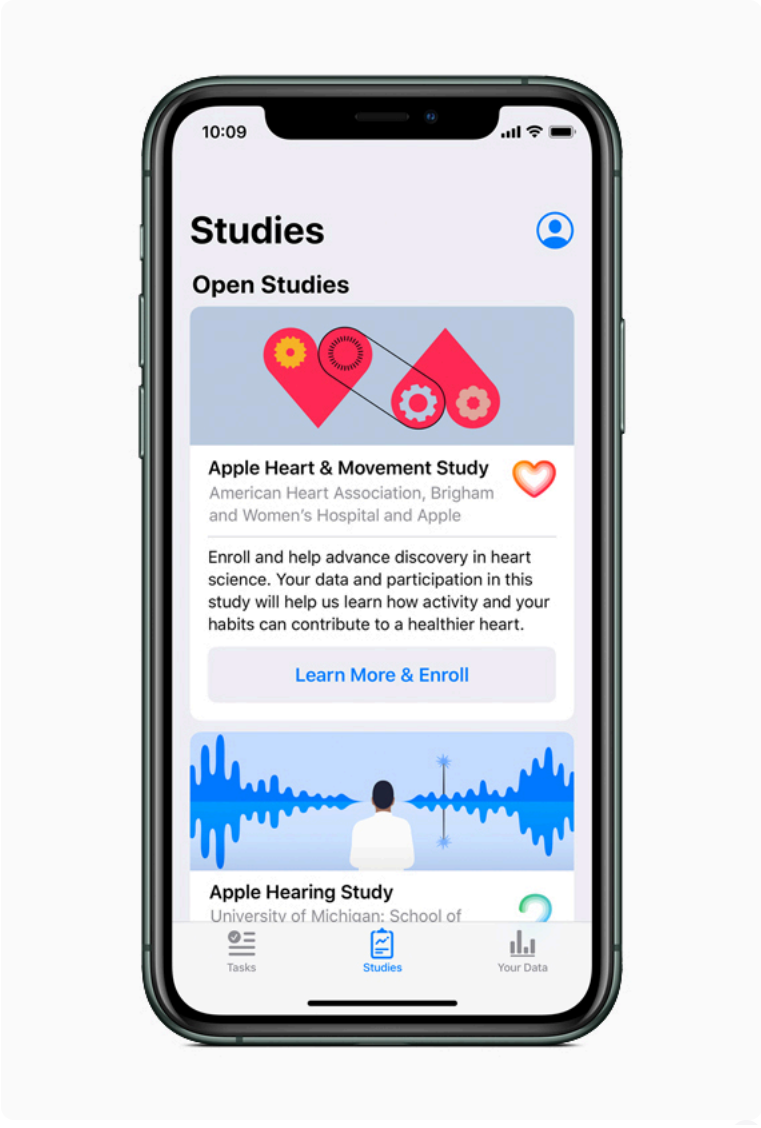
K. EXHIBIT K: APPLE.COM

Example of Apple's own website promoting its "menstruation" and "ovulation" software products and "studies" in 2019.
https://www.apple.com/newsroom/2019/09/apple-announces-three-groundbreaking-health-studies/]

UPDATE
September 10, 2019

Apple announces three groundbreaking health studies

In Collaboration with Leading Medical Institutions, Apple to Examine Hearing, Women's, Mobility and Heart Health



Three new studies, available on the Research app later this fall, will explore new areas of medical research.

Apple today announced three unprecedented medical studies, in partnership with leading academic and research institutions, that will reach more participants than has ever been possible. The studies will be available on the new Research app,[1] which democratizes how medical research is conducted by bringing together academic medical institutions, healthcare organizations and the Apple products customers already make a part of their everyday life. Participants will contribute to potential medical discoveries and help create the next generation of innovative health products. The Research app will be available as a free download in the App Store later this year.

"With the Apple Heart Study, we found that we could positively impact medical research in ways that help patients today and that make contributions that will benefit future generations," said Jeff Williams, Apple's chief operating officer. "Today's announcement carries our commitment to health even further by engaging with participants on a larger scale than ever before."



The Apple Heart and Movement Study will look into the connection of heart health and mobility signals, like walking pace.

The studies include:

- **Apple Women's Health Study**: In partnership with Harvard T.H. Chan School of Public Health and the NIH's National Institute of Environmental Health Sciences (NIEHS), Apple has created the first long-term study of this scale focused on menstrual cycles and gynecological conditions. This study will inform screening and risk

assessment of conditions like polycystic ovary syndrome (PCOS), infertility, osteoporosis, pregnancy and menopausal transition.

- **Apple Heart and Movement Study:** Apple is partnering with Brigham and Women's Hospital and the American Heart Association on a comprehensive study of how heart rate and mobility signals — like walking pace and flights of stairs climbed — relate to hospitalizations, falls, heart health and quality of life in order to promote healthy movement and improved cardiovascular health.

- **Apple Hearing Study:** Alongside the University of Michigan, Apple is examining factors that impact hearing health. The Apple Hearing Health Study is the first of its kind to collect data over time in order to understand how everyday sound exposure can impact hearing. The study data will also be shared with the World Health Organization (WHO) as a contribution toward its Make Listening Safe initiative.



The Apple Women's Health Study will explore gynecological conditions on an unparalleled scale.

Apple's support of the medical research community began with the introduction of ResearchKit and CareKit, which expanded the pace and scale at which healthcare could be studied and provided. Apple used ResearchKit to create the Apple Heart Study, which was the largest study of its kind and illustrated the impact virtual, large-scale studies can have on medical research by examining atrial fibrillation to provide validation for the irregular rhythm notification feature on Apple Watch.

"Women make up half of the world's population, yet even today there has been limited investment in studying their unique health needs,"

said Michelle A. Williams, a reproductive epidemiologist and dean of the faculty at the Harvard T.H. Chan School. "This study, unprecedented in scope, will greatly advance our understanding of the biological and social determinants of women's health, and lead to better health outcomes."

"This is an exciting opportunity for NIEHS researchers to contribute to the study design and use the resulting data to answer novel questions, not only important to women of reproductive age, but to women of all ages," said Dale Sandler, Ph.D., chief of the NIEHS Epidemiology Branch.

"We are excited to be working with all the study participants and with Apple to identify the features of complex human physiology that lead to different outcomes in wellness or chronic disease, and to use this information to empower individuals to maximize their own health," said Calum MacRae, the vice chair of Scientific Innovation for the Department of Medicine at Brigham and Women's Hospital and associate professor of Medicine at Harvard Medical School.

"At the American Heart Association, we are a relentless force for a world of longer, healthier lives, and we are committed to educating and empowering people to be proactive in all areas of their heart health and general well-being," said Nancy Brown, CEO of the American Heart Association. "We believe that emerging technology solutions that seek to provide deeper health insights offer great potential in getting us there. We are collaborating with Apple and Brigham and Women's Hospital on the Apple Heart and Movement Study to explore the correlation between a broad range of physical activities and a person's overall heart health to ultimately understand risks and interventions to improve health."

"We are excited about this unique opportunity to partner with Apple to determine how everyday activities affect our hearing," said DuBois Bowman, dean of the University of Michigan School of Public Health. "The information gleaned from this partnership will be critical for us to address the public health impact of various noise exposures on hearing loss in the United States."

"The World Health Organization is pleased to note the announcement of the Apple Hearing Study which will contribute toward our Make Listening Safe initiative by improving our understanding of users' listening behaviors," said Dr. Shelly Chadha, technical officer of Prevention of Deafness and Hearing Loss at the World Health Organization. "With over a billion young people who could be at risk of hearing loss due to unsafe listening, WHO is addressing this challenge through raising awareness and setting new standards for safe listening. The knowledge gained through this study will contribute to future public health action in this field."

Images of Apple Health Studies
Download all images

[1] Available in the US only.

Press Contacts

Apple Media Helpline
media.help@apple.com

Apple Media Helpline
media.uk@apple.com

More from Apple Newsroom



UPDATE

Formula 1® begins this weekend, exclusively on Apple TV in the U.S.

March 5, 2026



PRESS RELEASE

Say hello to MacBook Neo

March 4, 2026



PRESS RELEASE

Apple debuts M5 Pro and M5 Max to supercharge demanding pro workflows

March 3, 2026

Newsroom

The latest news and updates, direct from Apple.

Read more

Apple Books
App Store

Apple Wallet
Wallet
Apple Card
Apple Pay
Apple Cash

Shop for Veterans and Military
Shop for State and Local Employees
Shop for Federal Employees

Investors
Ethics & Compliance
Events
Contact Apple

More ways to shop: Find an Apple Store or other retailer near you. Or call 1-800-MY-APPLE (1-800-692-7753).

Copyright © 2026 Apple Inc. All rights reserved. Privacy Policy | Terms of Use | Sales and Refunds | Legal | Site Map United States | Español

L. EXHIBIT L: WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

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

INTRODUCTION **4**

APPLE'S CULTURE OF "LOYALTY" & INTIMIDATION 6

ELECTRONIC MONITORING & DATA COLLECTION **12**

"FACE ID"& APPLE'S FACE "GOBBLER" APPLICATION 12

EAR STUDIES 27

OTHER USER STUDIES 30

RADAR & SYSDIAGNOSE 32

SECRECY **33**

SECRECY POLICIES 33

SEARCH AND PRIVACY POLICIES 35

PUBLIC POLICY **40**

CONCLUSION **46**

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/

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

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

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

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.

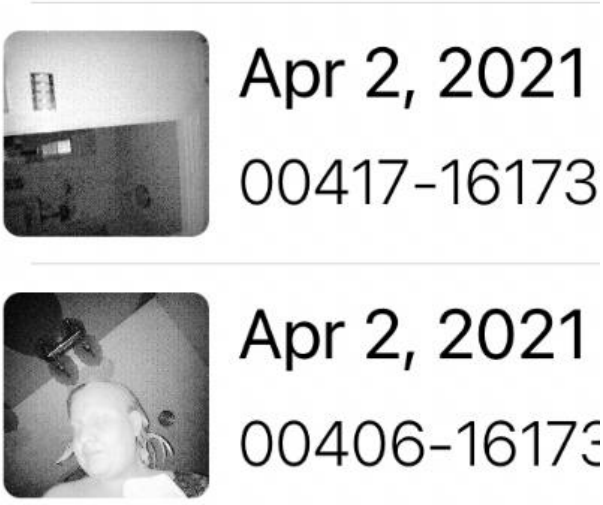


Figure 2: Photos captured by "Gobbler" in Gjovik's home bathroom, including Gjovik washing her face without clothing

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]

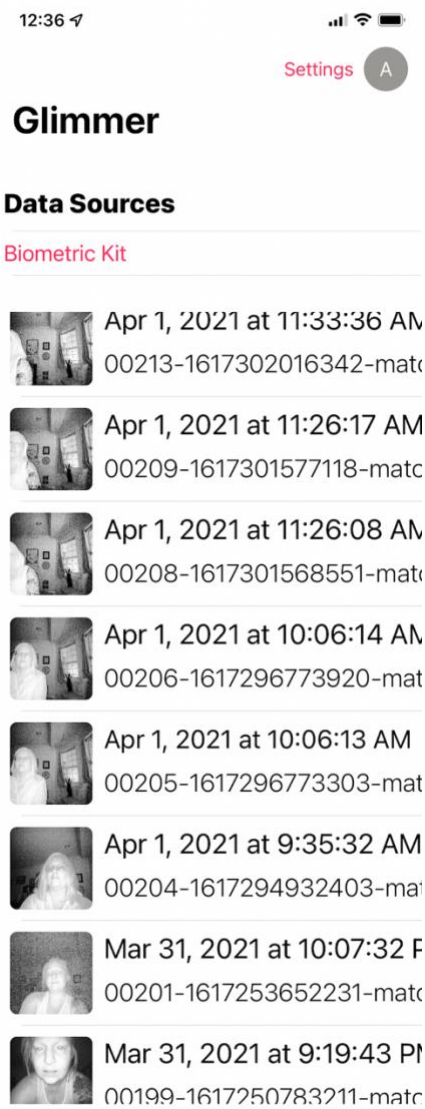
I also saw in notes that the app was forbidden to be used in Japan and China, but then at some point, Apple decided to gather some logs there anyways. On October 16, 2019 an engineer filed a Radar titled, "*Add Geo Location into Glimmer,"* saying

> *"*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?*

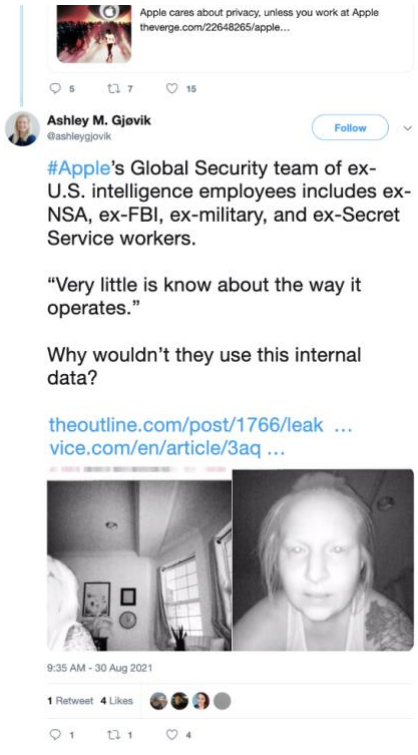
I partnered with a journalist to expose my concerns and the article was published on August 30, 2021 – while I was still employed by Apple, but while I had been forced on paid administrative leave. The article was titled, "***Apple Cares About Privacy, Unless You Work at Apple.***" [103] The article 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

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



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/1432416891201490 94

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



ASHLEY M. GJØVIK
@ashleygjovik

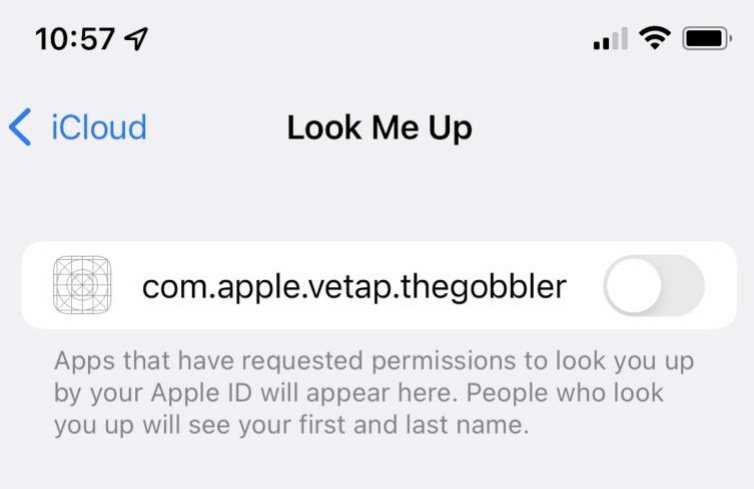
I still love #Apple products & brand. I devoted nearly 7 years & much blood/sweat/tears ensuring Apple's products are exceptional. However, Apple the corporation needs a reckoning. Apple's policy of "secrecy" should not shield it from public scrutiny about human rights & dignity.

> 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

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

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*

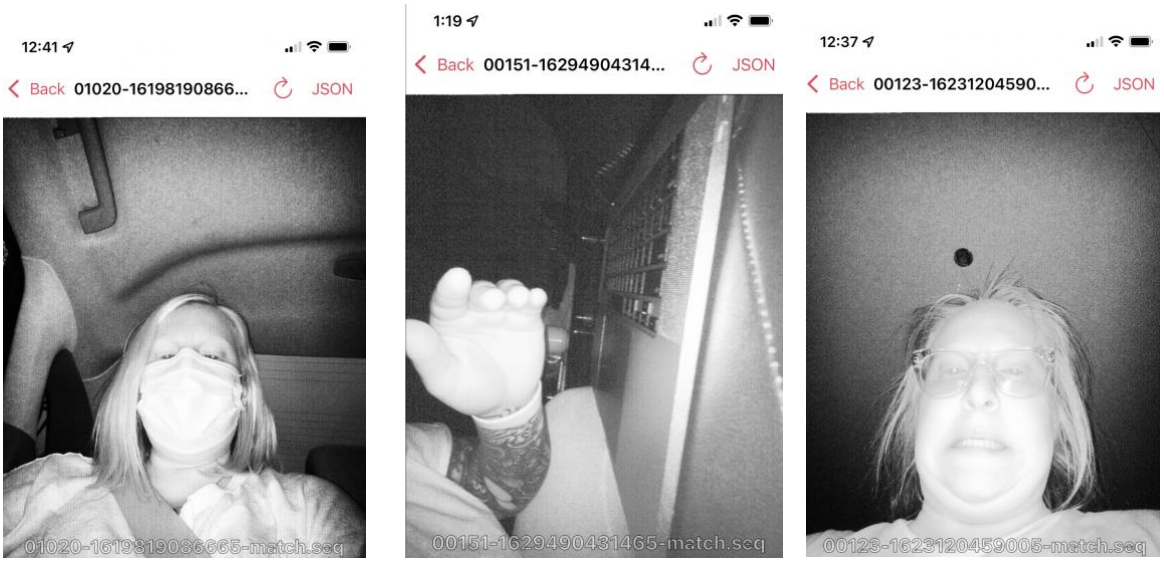
[124] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[125] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[126] Julie Samuels, *Steve Jobs Is Watching You: Apple Seeking to Patent Spyware*, EFF, Aug 23 2010
[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]

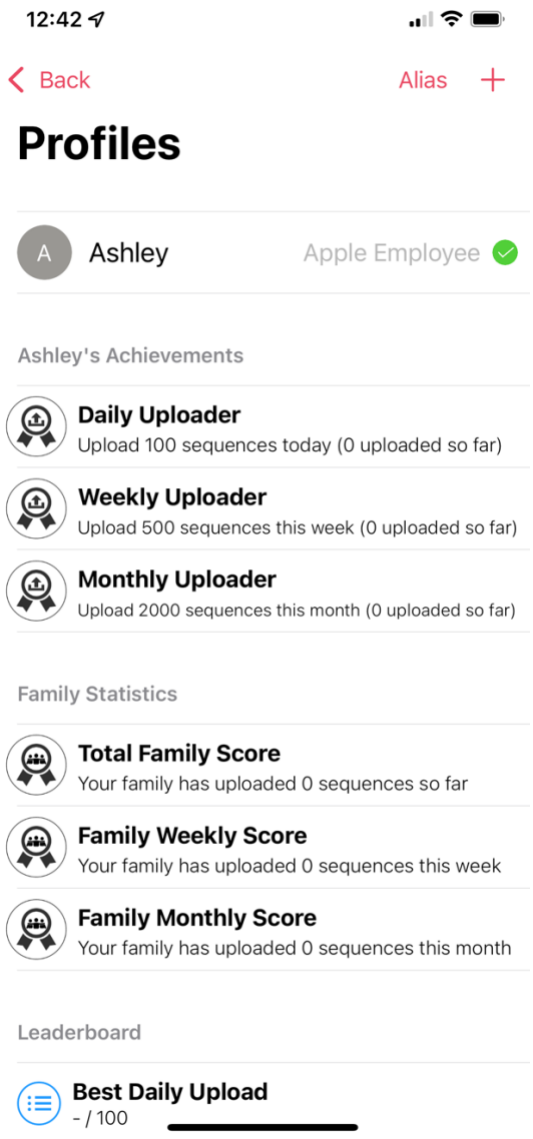
On March 4 2022 Apple (via Orrick lawyers) wrote to the U.S. federal government that:

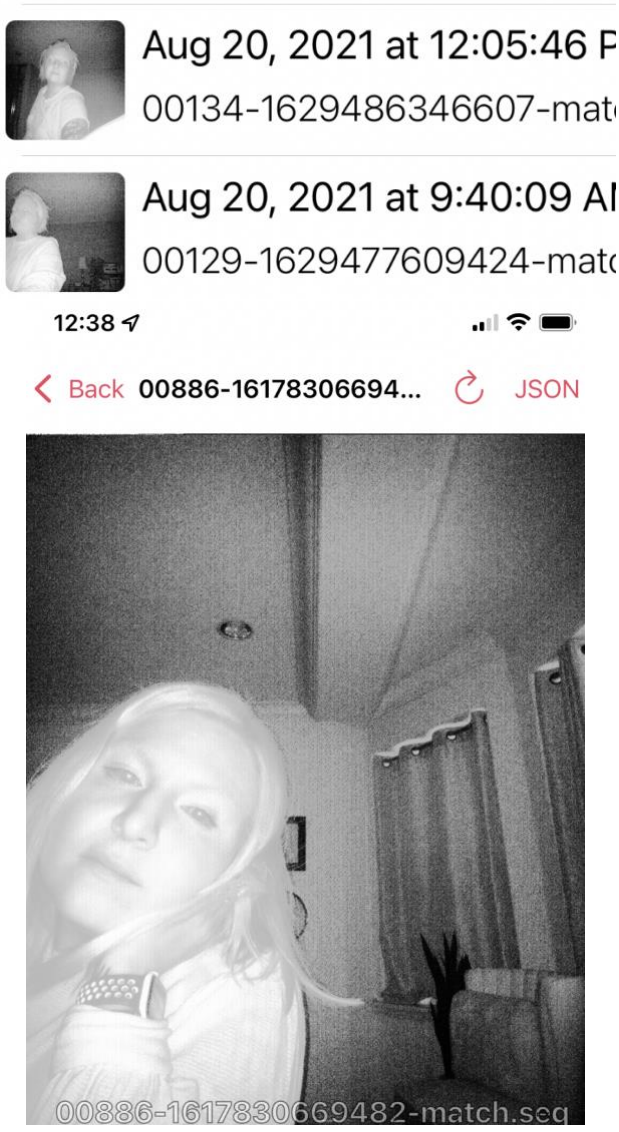
> "Apple terminate Ms. Gjovik's employment … because she violated Apple policy by intentionally disclosing confidential information about Apple products on Twitter and, as Apple later discovered, to the press … On August 30, 2021, Ms. Gjovik tweeted photographs and a video of herself created by the [Gobbler] 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]

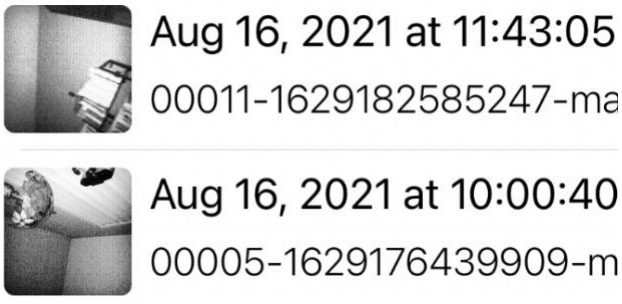


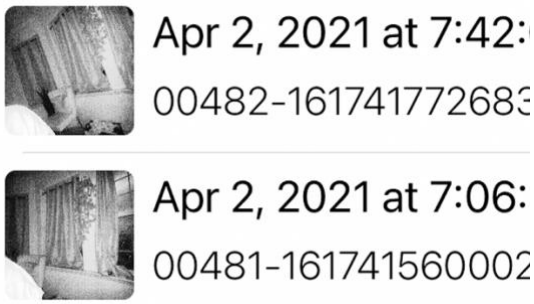
[132] Renee Oricchio, *Orwellian Watch: Apple's Creepy Patent Application*, Inc., https://www.inc.com/tech-blog/orwellian-watch-apples-creepy-patent-application.html
[133] 9to5 Staff, *Patent indicates sophisticated remote surveillance for Find My iPhone*, (Jun. 16th 2011), https://9to5mac.com/2011/06/16/patent-indicates-sophisticated-remote-surveillance-for-find-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"







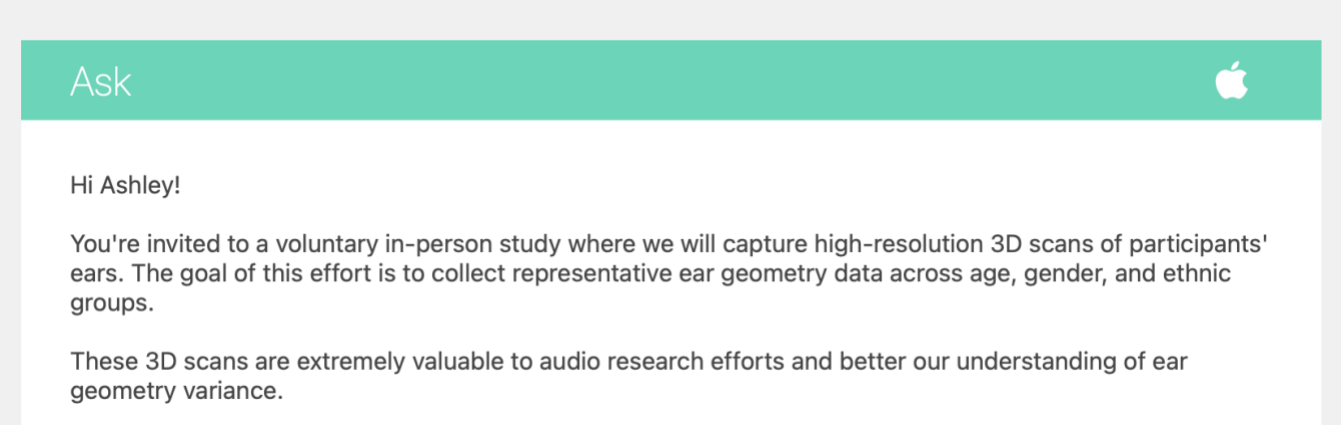


EAR STUDIES

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).



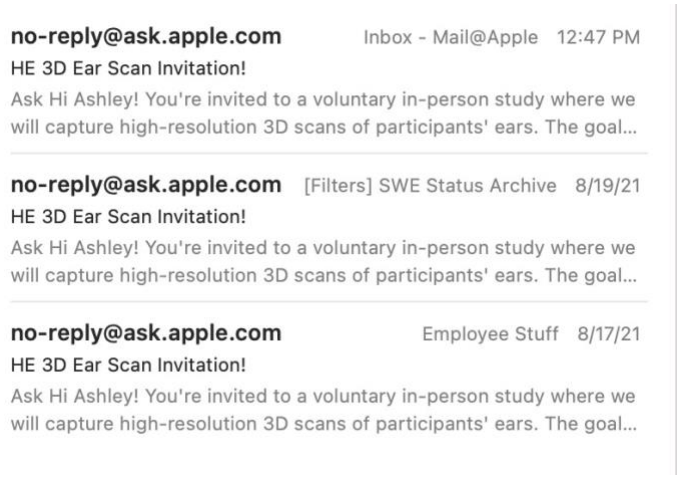
[136] Aug 10 2018, Gjovik to SJ
[137] Ask survey



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

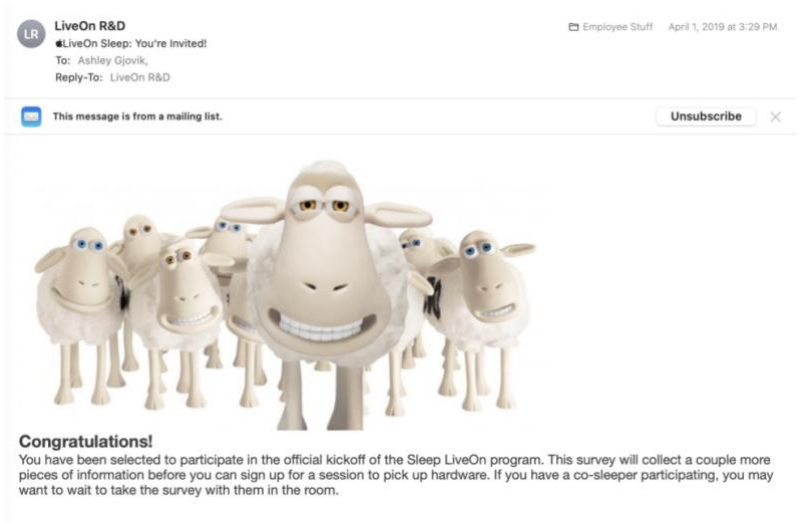
[143] Patent number 10856068
[144] Ahila Priyadharshini, R., Arivazhagan, S. & Arun, M. A deep learning approach for person identification using ear biometrics. *Appl Intell* **51,** 2161–2172 (2021). https://doi.org/10.1007/s10489-020-01995-8
[145] 3D Ear Biometrics BIR BHANU, HUI CHEN, Center for Research 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/

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

> "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).

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

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].

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

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/

M. EXHIBIT M: GOVERNMENT ACCOUNTABILITY OFFICE

Exhibit the Government Accountability Office Report GAO-24-107639, published August 28, 2024 and blog post published October 29, 2024, which references my public comment OSTP_FRDOC_0001-0008 in its findings

U.S. Government Accountability Office

Digital Surveillance of Workers: Tools, Uses, and Stakeholder Perspectives

GAO-24-107639

Q&A Report to Congressional Requesters

August 28, 2024

Why This Matters

A range of digital surveillance tools have been developed, and employers across various industries are increasingly using them to monitor their workers. Although digital surveillance tools can provide employers with information to help improve their operations, some worker advocates are concerned that these tools can be used in ways that negatively affect workers. We were asked to examine the kinds of digital surveillance tools employers use and how such surveillance affects workers.

This report summarizes 217 public comments submitted to the White House Office of Science and Technology Policy's request for information regarding use of automated digital surveillance tools to monitor workers and the effects of such surveillance on workers. Stakeholders submitted these comments from May to June 2023. We identified 211 stakeholders who submitted comments: 91 workers, 19 advocacy organizations, 16 researchers and research organizations, 12 unions, 10 trade associations, eight technology developers, one coalition comprised of advocacy organizations and a union, and 54 unspecified stakeholders.

These stakeholders submitted comments regarding various topics such as worker productivity, privacy, and safety.

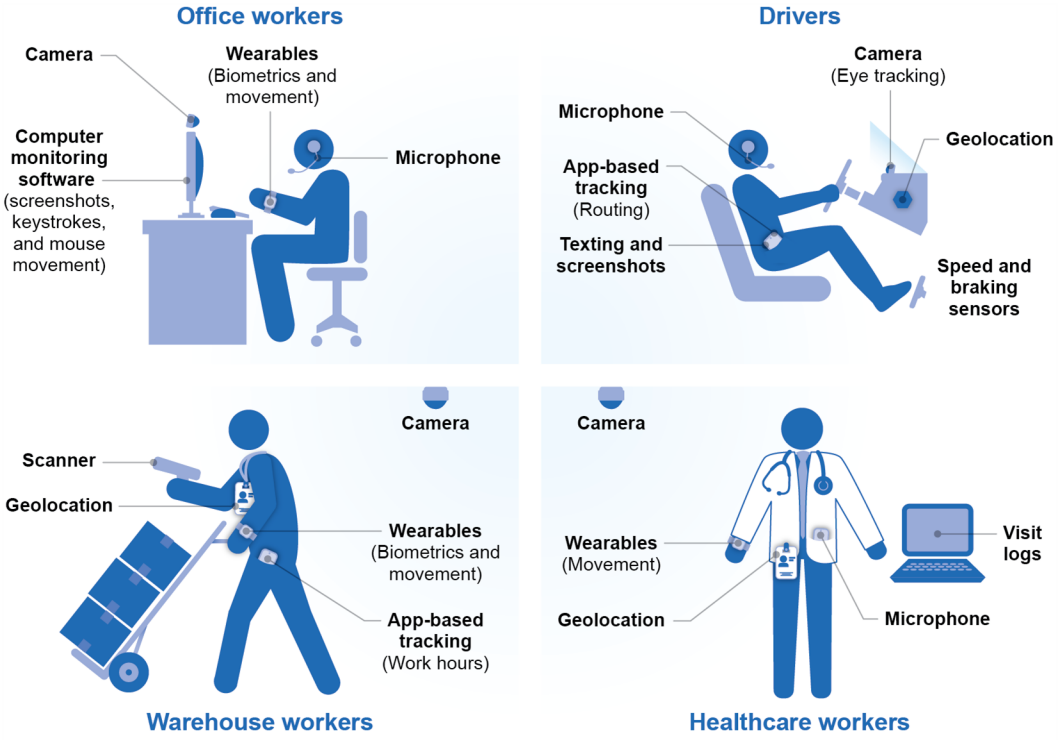
Key Takeaways

- The digital surveillance tools most frequently mentioned by stakeholders that employers use include cameras and microphones, computer monitoring software, geolocation, tracking applications, and devices worn by workers (wearables).
- Employers use digital tools to monitor (1) productivity and efficiency, (2) worker performance, (3) safety and health, and (4) workplace security.
- Stakeholders' views differed regarding the effects of digital surveillance on worker productivity and worker well-being.
- Workers and stakeholders from unions commented that digital surveillance may discourage workers from unionizing, make workers feel distrusted by their employers, and decrease workplace morale.
- Privacy was the most frequently raised concern by stakeholders and the potential for discrimination or bias was also a frequently raised concern.

What kinds of digital surveillance tools did stakeholders describe?

Stakeholders described an array of digital surveillance tools employers used to monitor workers across various industries (see fig. 1).[1]

Figure 1: Kinds of Digital Surveillance Tools Used in Various Workplaces



Source: GAO analysis of public comments submitted to the White House Office of Science and Technology Policy; GAO (icons). | GAO-24-107639

Note: GAO classified workers who perform most of their work on a computer (either in an office or remotely) as "office workers." This includes those who work in call centers, law, finance, banking, and technology, among others. The digital surveillance tools shown here are just some of those identified by stakeholders.

- **Cameras and microphones.** These video- and audio-monitoring tools were the most commonly mentioned by stakeholders. Specifically, 51 stakeholders commented that employers use cameras to monitor workers. Additionally, 22 commented that employers use audio-monitoring tools for purposes such as monitoring calls while at work (11 stakeholders mentioned both cameras and audio-monitoring tools). For instance, a company may record service representatives' phone calls for training purposes. These surveillance tools are used in sectors like warehousing, retail, healthcare, domestic service, call centers, and trucking.
- **Computer monitoring software**. This was the second most common type of digital surveillance tool, mentioned by 42 stakeholders. This software allows employers to track workers' keystrokes, mouse movements, eye movements, texts, and screenshots. In addition, stakeholders commented that the software allows employers to track workers' browser history, locations, attendance, and work activities. Stakeholders generally commented that this software is used to monitor office workers.
- **Geolocation software**. Thirty-three stakeholders commented that employers use this software to track their workers' location. This software can be installed on workers' personal phones to track their movements throughout the workday. It can also monitor vehicle speed, driving behavior, and routing. Geolocation tracking is used in industries such as long-haul trucking, delivery services, rideshare, gig work, healthcare, domestic service, and construction.
- **Tracking applications.** Thirty stakeholders commented that some employers use application-based tracking tools. These tools monitor workers' start and end times for work, body movements, speed of work, and activities. In these

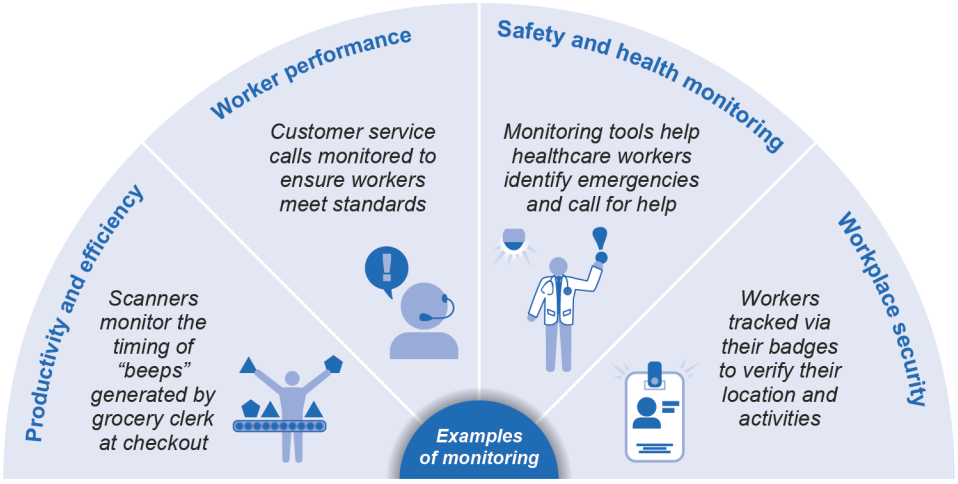
instances, employers require workers to download an application onto either their personal or company-provided cellphones or tablets. These applications give employers immediate information about workplace activities. According to stakeholders, application-based tracking is found in industries such as rideshare, warehousing, retail, and healthcare.

- **Wearables**. Twenty-seven stakeholders commented that employers may require workers to attach various forms of wearable technology to themselves for monitoring purposes. Electronic sensors embedded in these wearable devices track body movements, conversations, order processing, and biometric health data such as heart rate and blood pressure.[2] These tools can be found in warehouses, heavy industry, healthcare, and office settings.

What do these tools monitor?

Stakeholders commented that employers use digital tools to monitor (1) productivity and efficiency, (2) worker performance, (3) safety and health, and (4) workplace security (see fig. 2).

Figure 2: Example Uses of Digital Surveillance



Source: GAO analysis of public comments submitted to the White House Office of Science and Technology Policy; GAO (icons). | GAO-24-107639

- **Productivity and efficiency.** Seventy-six stakeholders commented that digital surveillance could be used to monitor worker productivity and efficiency. Productivity monitoring includes measuring the amount of work completed and whether workers are on task. For example, stakeholders from one research organization noted that increasing remote and hybrid work arrangements had raised employer concerns of workers avoiding their responsibilities. They commented that these changes had led employers to track keystrokes and webcams to evaluate productivity. Efficiency refers to whether workers are optimizing company time, money, and other resources. For example, one trade association commented that employers used digital surveillance to help establish economical work practices (see text box).

> **Comment from a trade association:**
> "Some [app-based] delivery platforms use [a worker's] location information as a tool for businesses, workers, and consumers. By leveraging such location information, from restaurant pick-up to customer dropoff, the platforms help drivers ensure they are in the right location and restaurants are able to time preparation more accurately."

Source: White House Office of Science and Technology Policy. | GAO-24-107639

- **Performance.** Sixty-four stakeholders commented that digital surveillance tools are used to determine the quality of work completed and whether workers are fulfilling their responsibilities appropriately and accurately. For

instance, stakeholders from one union commented that some truck drivers may be monitored for their driving behavior, such as whether their hands are on the wheel or if their eyes are facing forward. This data can be used to evaluate drivers' performance and may be used for disciplinary purposes in cases of distracted driving or if drivers do not complete their routes on time.

- **Safety and health.** Thirty-one stakeholders commented that employers may use digital surveillance to ensure worker safety and prevent accidents. Nine stakeholders commented that employers may use digital surveillance tools to assess their workers' health as they complete their responsibilities. For instance, stakeholders from a union commented that some employers require workers to wear monitors to collect data on workers' heart rate or blood pressure to evaluate mental or physical stress levels.
- **Security.** Thirteen stakeholders commented that digital surveillance can also be used to maintain security—ensuring only authorized personnel enter the workplace and preventing loss, theft, or waste of resources. For example, a researcher reported that facial recognition technology can monitor workers handling sensitive information and send alerts if an unauthorized person accesses the information.

How does digital surveillance affect worker productivity?

Stakeholders' views differed regarding the effect of digital surveillance on worker productivity. Researchers and stakeholders from unions and advocacy organizations commented that it is difficult to know its effects because digital surveillance tools may not accurately measure productivity. However, other stakeholders offered differing views on how digital surveillance affects worker productivity. For example, trade associations and researchers commented that digital surveillance increases worker productivity. In contrast, other stakeholders said that it reduces worker productivity.

- **Possible inaccurate measures of productivity**. Thirty-one stakeholders, including researchers and stakeholders from unions and advocacy organizations, commented that digital surveillance tools may provide an incomplete or inaccurate measure of productivity. For example, stakeholders from a research organization and an advocacy organization commented that employers may not be fully capturing workers' performance because some tasks may be completed offline or are not easily traced. Also, a worker advocacy organization commented that digital surveillance tools that measure how long a worker takes to complete tasks may not accurately account for things such as breaks and accommodations needed for injuries.
- **Differing views about effects on worker productivity.** Sixteen stakeholders, including trade associations, researchers, and a technology developer, commented that digital surveillance increases worker productivity. For instance, stakeholders from one trade association commented that digital surveillance allows employers to identify specific areas for improvement and provide targeted coaching, training, and other support. In contrast, nine stakeholders, including those from advocacy organizations, workers, and researchers, commented that digital surveillance reduces productivity. For example, a researcher commented that workers frequently take on insignificant or meaningless tasks to meet metrics that make them appear productive. This can include jiggling a mouse so it is registered by monitoring software.

How does digital surveillance affect workers' relationships with their employers?

Workers and stakeholders from unions commented that digital surveillance may discourage workers from unionizing and make workers feel distrusted by their employers. They also commented that it can decrease workplace morale.

- **May discourage unionizing efforts.** Thirty-one stakeholders, including workers and stakeholders from unions and research organizations, commented that digital surveillance may discourage unionizing efforts. One researcher commented that by monitoring and collecting data on workers, employers compile information that can be used to deter unionization. Several stakeholders from unions, advocacy organizations, and research organizations commented that employers in many industries use digital surveillance tools to identify and monitor workers who engage in labor organizing and union activity.
- **Feeling distrusted by employers.** Twenty stakeholders commented that digital surveillance may make workers feel distrusted by employers, with nine workers specifically commenting they felt that their employers did not trust them. Stakeholders from an advocacy organization, a union, and a researcher commented that due to monitoring, some workers have become more hesitant to voice their concerns about workplace issues, fearing that their digital activity will be used against them. One researcher highlighted a "negative spiral" in which employer distrust demotivated workers and adversely affected productivity.
- **Decreased workplace morale.** Nineteen stakeholders, including several unions, commented that digital surveillance can have a negative effect on workers' morale. For example, a researcher commented that workplace morale decreases when workers who are monitored worry about how their productivity scores will affect their pay. One union said that heightened expectations on employees combined with frequent and secretive surveillance has had significant negative impacts on their morale.

How does digital surveillance affect worker well-being?

Stakeholders commented that digital surveillance has mixed effects on worker well-being. Workers and researchers commented that digital surveillance tools had negative effects on mental health and generally negative effects on workplace safety. In contrast, stakeholders, including researchers and stakeholders from advocacy organizations, commented that these tools had a positive effect on workplace security. Additionally, stakeholders, including trade associations, commented that these tools had a positive effect on preventing illness.

- **Negative effects on mental health.** Fifty-nine stakeholders, including workers, researchers, unions, and advocacy organizations commented that digital surveillance decreased workers' mental health (see text box). Workers reported that digital surveillance increased stress and fear. Advocacy organizations also said that digital surveillance increased anxiety and depression among workers. A researcher commented that performance-scoring technologies can increase workers' stress and the risk of mental health problems. Specifically, they commented that when an employer turns productivity-scoring systems into "games" that pit workers against each other by making their productivity metrics public, workers' stress increases.

Comment from a call center agent:
"All of these tools are often used to drive an unrelenting push for sales . . . This pressure to sell and the various ways that managers can monitor me creates an enormous amount of stress. Over the past few years in this position, the stress has made me sick to my stomach and unable to get out of bed in the morning to do my job. I've started taking [medical leave] as a result of missing workdays due to stress."

Source: White House Office of Science and Technology Policy. | GAO-24-107639

- **Generally negative comments about effects on workplace safety.** Forty-nine stakeholders, including workers and stakeholders from advocacy organizations, commented that digital surveillance tools can reduce safety. For example, some stakeholders commented that these tools increase the pace at which workers must complete tasks, and therefore can make tasks more dangerous. Conversely, 15 stakeholders, including an advocacy organization and several trade associations, commented that digital surveillance tools can increase safety by reducing accidents and injuries. For instance, stakeholders from a trade association commented that employers may use digital surveillance tools, such as wearable technology, to detect ergonomic risks, toxic or combustible liquids or gases, and other hazards.
- **Positive effects on workplace security.** Twelve stakeholders, including researchers and stakeholders from trade associations, unions, and an advocacy organization, commented that digital surveillance tools improved workers' well-being by preventing workplace violence and increasing workplace security (see text box). One of these stakeholders commented that digital surveillance tools, such as those that detect intruders, can protect workers from harm and improve emergency responses. For example, rideshare platforms monitor for instances of unusual activities, such as long stops, which may be an indication of an emergency. A trade association also commented that digital surveillance tools can enhance workplace security by deterring potential criminal activity such as workplace violence, theft, and security breaches.

Comment from a labor union:
"[The union] has also negotiated to ensure that hotel housekeepers have GPS-enabled panic buttons to alert hotel security if they feel unsafe or threatened, a not uncommon occurrence for housekeepers who have faced sexual harassment and assault from hotel guests."

Source: White House Office of Science and Technology Policy. | GAO-24-107639

- **Positive effects on illness prevention.** Four stakeholders—two trade associations, a union, and an advocacy organization—commented that employers use digital surveillance tools to prevent or reduce illness. One trade association commented that digital surveillance enabled employers to enforce relevant health protocols during the COVID-19 pandemic (see text box). Another trade association commented that digital surveillance tools, such as heat stress monitors, can reduce workers' risk of heat-related illnesses.

Comment from a trade association:
"During COVID-19, the use of automated systems has enabled individuals to work safely by helping employers utilize cameras, sensors, and augmented reality to create important social-distancing tools and enforce relevant health protocols."

Source: White House Office of Science and Technology Policy. | GAO-24-107639

What concerns did stakeholders report about the use of these tools regarding privacy?

Stakeholders generally described privacy concerns regarding the information employers collect on workers' digital activities (digital privacy) and bodies (bodily privacy). Privacy was the most frequently raised concern by stakeholders, with 87 stakeholders commenting about this issue.

- **Digital privacy.** Seventy-three stakeholders, including workers, researchers, and stakeholders from unions and advocacy organizations, commented that digital surveillance tools can monitor workers' digital information through their personal or company-owned devices. Stakeholders from a union federation described some employers requiring remote workers to download software that gave managers access to their computer cameras and microphones while they were at home. A worker reported being fired from a large technology company after raising concerns about the company's privacy policy, which empowered managers to access, search, monitor, archive, and delete data stored on any worker's devices. Four stakeholders, including one researcher, two advocacy organizations, and a union, commented that employers may monitor workers' social media posts to identify workers who may be involved in labor organizing activities.
- **Bodily privacy.** Thirty-three stakeholders, including workers, unions, researchers, and advocacy organizations, commented that employers collect information related to workers' bodies. This could include biometric measurements or recordings of voices. For example, some employers record videos, watch employees via cameras, access their microphones, or record their voices on personal devices. Others collect biometric and health data through wearable technology or phone applications, including those that can track menstruation. While some stakeholders from trade associations commented that biometric data collection can help improve workplace safety and employee well-being, unions, workers, and advocacy organizations commented that such surveillance violates workers' privacy.

What concerns did stakeholders report about the potential for discrimination or bias due to the use of digital surveillance?

The potential for discrimination or bias was also among the most frequently raised concerns by stakeholders. Sixty-three stakeholders, including advocacy organizations, researchers, and unions, identified the potential for such discrimination or bias based on several characteristics including race, gender and pregnancy, or disability.

- **Race.** Twenty-nine stakeholders commented that digital surveillance could lead to potential discrimination or bias toward workers based on race. Stakeholders from an advocacy organization commented that when digital surveillance is used to monitor employee performance—especially if it requires customer reviews—racial bias can lead to negative outcomes for racial minorities. This organization also commented that rideshare drivers rely on online customer ratings to earn wages and maintain their employment on application-based platforms. Additionally, if a driver consistently receives low customer service ratings due to potential racial bias from passengers, the driver risks getting removed from the rideshare platform. Further, this advocacy organization commented that minority drivers are more likely to be suspended from rideshare platforms due to customer service complaints.
- **Gender and pregnancy.** Twenty-one stakeholders commented that digital surveillance could lead to potential discrimination or bias against women or pregnant workers. For example, stakeholders from one research and one advocacy organization commented that a wellness app used by employers gathered information about menstruation, fertility, and pregnancy. Stakeholders from the advocacy organization commented that an employer

with access to that information could terminate or fail to promote an individual before they disclose their pregnancy status to their employer.

- **Disability.** Twelve stakeholders commented that digital surveillance could lead to potential discrimination or bias toward workers with disabilities. Stakeholders commented that workers with disabilities may need more time to complete tasks, and digital surveillance that monitors their productivity may flag them as low performers. According to stakeholders from an advocacy organization, individuals with certain disabilities or chronic illnesses that cause delays in cognitive processes and physical activities may require more time to complete tasks (see text box). Other stakeholders commented that employers using digital surveillance often consider whether the worker can maintain the pace of work in their role when evaluating productivity and performance. One stakeholder commented that time used for a bathroom break is considered by employers to determine productivity. This could negatively affect the perceived performance of workers with disabilities, who may require more time for bathroom breaks.

Comment from a coalition of worker advocacy organizations:

"[Electronic surveillance combined with automated management] poses unique risks that threaten to exacerbate the disadvantages that pregnant and disabled workers already face. One of the most common uses of [this technology] is to increase the pace of work, discouraging workers from taking breaks or downtime and often penalizing them for doing so. Such practices may discriminate against disabled and pregnant workers, who may be more susceptible to new and aggravated injuries and illnesses in the workplace and are expected to comply with arbitrary, automatically enforced standards that do not consider disability- and pregnancy-related needs that may require opportunities for rest, flexibility, and supportive work environments. Workers with gastrointestinal and urinary tract disorders, for example, may need to use the restroom more frequently or at unpredictable times."

Source: White House Office of Science and Technology Policy. | GAO-24-107639

What concerns did stakeholders report about workers' knowledge of how employers use data collected through digital surveillance?

Advocacy organizations, researchers, unions, and workers commented that workers do not understand how employers use data they collect from digital surveillance to make decisions.

- **Lack of transparency**. Forty-five stakeholders, including workers, advocacy organizations, researchers, and unions, commented that there is a lack of transparency about employers' use of digital surveillance (see text box). For example, eight workers commented that their employers are not forthright about how they use workers' data to evaluate them or make job-related decisions. Two workers and a research organization commented that even when they are required to download digital surveillance tools onto their personal devices, employers are not transparent about what information they collect or how they use the information.

Comment from a technology worker:

"I was sent a company computer with a webcam and required to have it on at all times (except for breaks). The computer requires me to log in to my user profile . . . I am required to scan my facial biometrics. Once the lengthy verification login process is done, I am on camera all day. The webcam monitoring software uses [Artificial Intelligence] AI to track what is caught on camera, looking for violations. Certain violations are known to us, such as pointing [a] phone at [the] screen or leaving the desk, but no further information is told to us about all violations the AI is looking for and what else is the AI tracking."

Source: White House Office of Science and Technology Policy. | GAO-24-107639

How GAO Did This Study

We analyzed public comments submitted to the White House Office of Science and Technology Policy (OSTP) in response to a request for information regarding experiences with the use of automated worker surveillance and management.[3] OSTP requested information from the public—including private and public sector workers—to better understand the prevalence, uses, purposes, and deployment of automated digital surveillance tools, including effects of these tools on workers' physical and mental health, privacy, and ability to exercise workplace rights.

OSTP's comment period ran from May 3 through June 29, 2023. In its request for public comments, OSTP noted that it was particularly interested in hearing from workers who have experienced automated digital surveillance; unions and advocacy organizations; employers, operators of virtual platforms, and other entities that match workers with opportunities to generate income; trade and business associations; researchers; and developers and vendors who manufacture or sell this type of technology, among others.

This report is the first of two reports on digital surveillance of workers. It summarizes 217 public comments submitted to OSTP through a request for information on the use of automated digital surveillance tools to monitor workers and the effect of such surveillance on workers. In the second report, we will incorporate stakeholder interviews and a literature search to enhance the information related to the impacts and uses of digital surveillance. Additionally, we will address how federal agencies oversee employers' use of digital surveillance technology.

For this report, we used a multistep process to analyze stakeholders' comments. This included: transferring the comments into a qualitative analysis software program; identifying themes in the comments and creating categories based on these themes; establishing agreement among the three analysts who reviewed the comments about how to categorize them into these themes; and having a fourth analyst verify that the comments were categorized correctly. We analyzed these comments to identify the types of digital surveillance tools stakeholders reported using. We also analyzed the comments to examine the types of workers who were monitored with these tools, how these tools were being used, and their effect on workers.

We conducted our work from June 2024 to August 2024 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for the information we report in this product.

List of Addressees

The Honorable Robert P. Casey, Jr.
Chairman
Special Committee on Aging
United States Senate

The Honorable Robert C. “Bobby” Scott
Ranking Member
Committee on Education and the Workforce
House of Representatives

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 29 days from the report date. At that time, we will send copies to the appropriate congressional committees and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

GAO Contact Information

For more information, contact: Thomas Costa, Director, Education, Workforce, and Income Security, CostaT@gao.gov, (202) 512-4769.

Sarah Kaczmarek, Acting Managing Director, Public Affairs, KaczmarekS@gao.gov, (202) 512-4800.

A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400.

Staff Acknowledgments: Mary Crenshaw (Assistant Director), Hedieh Fusfield (Analyst in Charge), Sarika Akula, James Bennett, John Bornmann, Dustin Cohan, Yasmine Evans, Lauren Kirkpatrick, Gabriel Nelson, Stacia Odenwald, Aaron Olszewski, and Kathleen van Gelder.

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.

Visit GAO on the web at https://www.gao.gov.

This is a work of the U.S. government but may include copyrighted material. For details, see https://www.gao.gov/copyright.

Endnotes

[1]We counted stakeholders as workers if they identified themselves as a worker or we inferred that they were a worker based on their comment. Specifically, we inferred that they were workers if they described their experiences or perspectives about digital surveillance that they encountered at work.

[2]For more information on wearable technology, see GAO, *Science & Tech Spotlight: Wearable Technologies in the Workplace,* GAO-24-107303 (Washington, D.C.: March 2024). We reported that certain wearables could reduce the risk of injuries from strenuous work or worker-equipment collisions and may improve response time to emergencies but concerns about privacy, cost, and ease of use may hinder widespread adoption.

[3]Request for Information; Automated Worker Surveillance and Management, 88 Fed. Reg. 27,932 (May 3, 2023).



'Why do I feel like somebody's watching me?' Workplace Surveillance Can Impact More Than Just Productivity

Posted on October 29, 2024

Do you ever get that eerie feeling like someone's watching you at work?

In today's digital world, employers are increasingly using digital surveillance tools to monitor workers. While many employers say that digital surveillance has benefits like increasing worker productivity, most workers say being watched gives them the creeps.

The question is—does this constant monitoring actually work? Does it increase productivity and safety, or is it killing morale and causing other issues?

For Halloween, today's WatchBlog post answers these and other questions, while looking at our new report about digital surveillance tools.



Source: stnazkul/stock.adobe.com.

Cameras, microphones, and tracking software—oh my! Why do employers like "bossware?"

Often referred to as "bossware," a wide range of digital surveillance tools are used in all kinds of workplaces. These include warehousing, retail, trucking, health care, and banking, to name just a few.

Digital Surveillance tools include everything from cameras, microphones, and computer monitoring software to advanced tracking software (like GPS), app-based monitoring, and even wearable devices that track workers' health data.



Why do employers like digital surveillance? The primary aim of digital surveillance is to monitor workers' productivity, performance, and efficiency. It allows employers to identify specific areas for improvement and provide targeted coaching, training, and other support. Some employers began using surveillance tools after increasing workplace flexibilities for their staff, such as remote and hybrid work arrangements. Employers who allow telework have raised concerns that workers are slacking off when working from home. Digital surveillance tools allow employers to check whether

their staff are working from where they say they are (and not… the beach, for example).

Some employers said they also use digital surveillance tools to increase workplace safety and health. For example, in oil production, one employer uses wearable devices to track workers' sweat levels and electrolyte loss to help prevent heat stress on the job.

Digital surveillance also bolsters security to ensure that only authorized personnel enter sensitive areas. With innovations like facial recognition technology, employers can swiftly respond to potential threats, creating safer working environments. For example, a labor union official commented that GPS-enabled panic buttons are used for hotel housekeepers to "alert hotel security if they feel unsafe or threatened, a not uncommon occurrence for housekeepers who have faced sexual harassment and assault from hotel guests."

Even with these potential benefits, employers weren't always sure how effective their tools were. For example, perpetual monitoring had led some workers to game the system—performing meaningless tasks, like jiggling a mouse, just to meet arbitrary milestones. And the constant monitoring is leading to negative effects on workers, which may outweigh some benefits.

Under constant scrutiny—why do workers dislike surveillance tools?

Digital surveillance tools are putting employees on edge and having other negative effects that could impact their mental health, morale, productivity, and more.

- **Worsens mental health:** Constant surveillance can amplify workers' stress and anxiety levels, making them feel like they're under a microscope. The sheer act of surveillance can contribute to workers' feeling less confident or enthusiastic about their jobs. Workers increasingly reported feeling that they cannot voice concerns or share suggestions out of fear that their digital footprint will bite back. When the work environment makes workers feel scrutinized, it may very well foster a culture of distrust.

  For example, a call center worker said that surveillance tools have resulted in an unrelenting push to improve sales. They said, "The pressure to sell and the

various ways that managers can monitor me creates an enormous amount of stress."

- **Discourages unionization:** Being perpetually watched can also eat away at a workers' sense of autonomy and privacy. Consequently, some workers feel it discourages workplace solidarity and unionization efforts. When workers fear their every move is being tracked, organizing for better conditions feels risky—undermining solidarity and weakening workplace morale.

- **Potential to create discrimination:** Workers' advocates and researchers worry about the potential for digital surveillance to create bias or discrimination. Some worry that AI-driven performance metrics might unfairly target certain groups. For instance, those who take longer to complete tasks due to disability or other factors. This could magnify existing disability, racial, or gender inequalities in the workplace.

For more spooky details, read our new report.

- GAO's fact-based, nonpartisan information helps Congress and federal agencies improve government. The WatchBlog lets us contextualize GAO's work a little more for the public. Check out more of our posts at GAO.gov/blog.

Topics

Employment | Department of Labor | Occupational Safety and Health Administration | Workplace safety and health | Worker protections | Worker safety | Electronic surveillance | Education, Workforce, and Income Security

GAO Contacts



Thomas Costa
Director
Education, Workforce, and Income Security
costat@gao.gov

Related Posts



orodenkoff/stock.adobe.com.

Blog Post

As Online Shopping Increases, So Do Concerns About Delivery and Warehouse Workers' Safety

WEDNESDAY, OCTOBER 9, 2024

Next-day delivery. Overnight shipping. Online sales in the U.S. have nearly doubled in the last few...



lalfpoint/stock.adobe.com.

Blog Post

How Can the Federal Government Strengthen its Response to the COVID-19 Pandemic?

WEDNESDAY, OCTOBER 27, 2021

Deep into the second year of the COVID-19 pandemic, from health care to the economy, challenges...



Source: Pond5

Blog Post

Vaccine Distribution, Supply Chain, Testing Still Present Challenges in Federal Pandemic Response

THURSDAY, JANUARY 28, 2021

Since November 2020, the number of COVID-19 cases in the U.S. has dramatically increased, further...

Related Products

Digital Surveillance of Workers: Tools, Uses, and Stakeholder Perspectives

GAO-24-107639

Published: Aug 28, 2024

Publicly Released: Sep 11, 2024

ABOUT THE WATCHBLOG

GAO's mission is to provide Congress with fact-based, nonpartisan information that can help improve federal government performance and ensure accountability for the benefit of the American people. GAO launched its WatchBlog in January, 2014, as part of its continuing effort to reach its audiences—Congress and the American people—where they are currently looking for information.

The blog format allows GAO to provide a little more context about its work than it can offer on its other social media platforms. Posts will tie GAO work to current events and the news; show how GAO's work is affecting agencies or legislation; highlight reports, testimonies, and issue areas where GAO does work; and provide information about GAO itself, among other things.

Please send any feedback on GAO's WatchBlog to blog@gao.gov.

Receive GAO Updates

Stay informed as we add new reports & testimonies.

Enter Your Email Address

SUBSCRIBE

N. EXHIBIT N: NLRB

NLRB National Settlement Agreement, Case No. 32-CA-284428

FORM NLRB-4722

NOTICE TO EMPLOYEES

POSTED PURSUANT TO A SETTLEMENT AGREEMENT APPROVED BY A REGIONAL DIRECTOR OF THE NATIONAL LABOR RELATIONS BOARD

AN AGENCY OF THE UNITED STATES GOVERNMENT

THE NATIONAL LABOR RELATIONS ACT GIVES YOU THE RIGHT TO:

- Form, join, or assist a union;
- Choose a representative to bargain with us on your behalf;
- Act together with other employees for your benefit and protection;
- Choose not to engage in any of these protected activities.

WE WILL NOT interfere with, restrain, or coerce you in the exercise of the above rights.

YOU HAVE THE RIGHT to discuss wages, hours and working conditions and **WE WILL NOT** do anything to interfere with your exercise of that right.

WE WILL NOT promulgate, maintain, or enforce any rule that defines confidential information as "anything not explicitly, publicly, or purposefully disclosed by Apple."

WE WILL NOT promulgate, maintain, or enforce a Confidentiality and Intellectual Property Agreement, Business Conduct Policy, Misconduct and Discipline Policy, Social Media and Online Communications Policy, Confidentiality Obligations Upon Termination of Employment statement, or a Business Conduct and Global Compliance FAQ regarding confidential information that broadly defines "confidential" or "proprietary" information, or relies upon any other overly broad definitions of those terms, without contemporaneously notifying employees of their rights to discuss wages, hours, or working conditions and their rights to engage in union or other protected, concerted activity under the NLRA.

WE WILL NOT promulgate, maintain, or enforce a Business Conduct Policy that broadly restricts public speaking, responses to press inquiries and publishing articles without contemporaneously notifying employees of their rights to speak publicly, respond to press inquiries and publish articles regarding their wages, hours, or working conditions, or their union or other protected, concerted activity under the NLRA.

WE WILL NOT promulgate, maintain, or enforce a Business Conduct Policy that broadly restricts "conflicts of interest" or "outside activities," without contemporaneously notifying employees that such policies do not restrict their right to form, join or assist a union, or engage in other protected, concerted activity and that these activities are not considered to be conflicts of interest or outside activities under such policy.

WE WILL NOT promulgate, maintain, or enforce a Business Conduct Policy that broadly prohibits sharing of employee personal identifying information if such policy could be interpreted as prohibiting the sharing of personal contact information, employment history, compensation or other terms and conditions of employment.

WE WILL NOT promulgate, maintain, or enforce a Workplace Searches and Privacy Policy that advises you that we have the right to access Apple's network or systems, or any non-Apple device used to conduct Apple business, without contemporaneously advising you that we will not exercise our right of access to monitor your union or other protected, concerted activity.

The National Labor Relations Board is an independent Federal agency created in 1935 to enforce the National Labor Relations Act. We conduct secret-ballot elections to determine whether employees want union representation and we investigate and remedy unfair labor practices by employers and unions. To find out more about your rights under the Act and how to file a charge or election petition, you may speak confidentially to any agent with the Board's Regional Office set forth below or you may call the Board's toll-free number 1-844-762-NLRB (1-844-762-6572). Hearing impaired callers who wish to speak to an Agency representative should contact the Federal Relay Service (link is external) by visiting its website at https://www.federalrelay.us/tty (link is external), calling one of its toll free numbers and asking its Communications Assistant to call our toll free number at 1-844-762-NLRB.

THIS IS AN OFFICIAL NOTICE AND MUST NOT BE DEFACED BY ANYONE.

THIS NOTICE MUST REMAIN POSTED FOR 60 CONSECUTIVE DAYS FROM THE DATE OF POSTING AND MUST NOT BE ALTERED DEFACED OR COVERED BY ANY OTHER MATERIAL. ANY QUESTIONS CONCERNING THIS NOTICE OR COMPLIANCE WITH ITS PROVISIONS MAY BE DIRECTED TO, THE ASSISTANT TO THE REGIONAL DIRECTOR NATHAN SEIDMAN AT nathan.seidman@nlrb.gov or (213) 634-6518. **PANEL 1 OF 3**

32-CA-284428

FORM NLRB-4722

NOTICE TO EMPLOYEES

POSTED PURSUANT TO A SETTLEMENT AGREEMENT APPROVED BY A REGIONAL DIRECTOR OF THE NATIONAL LABOR RELATIONS BOARD

AN AGENCY OF THE UNITED STATES GOVERNMENT

THE NATIONAL LABOR RELATIONS ACT GIVES YOU THE RIGHT TO:

- Form, join, or assist a union;
- Choose a representative to bargain with your employer on your behalf;
- Act together with other employees for your benefit and protection;
- Choose not to engage in any of these protected activities.

WE WILL NOT promulgate, maintain, or enforce a Misconduct and Discipline Policy that fails to reiterate employee rights during investigations that Apple may conduct regarding alleged unfair labor practices under the National Labor Relations Act, and/or contains overly broad restrictions on photography and recording.

WE WILL NOT advise you that you are subject to discipline for violating overly broad rules regarding confidential or proprietary information or for failing to report alleged violations of overly broad rules relating to confidential or proprietary information.

WE WILL NOT advise you that you are subject to discipline for violating overly broad rules regarding photographing, video or audio recording that prohibit the recording of protected, concerted activity.

WE HAVE clarified the aspects of the Confidentiality and Intellectual Property Agreement described above and revised it to make clear that the definition of "Proprietary Information," which was changed to "Apple Confidential Information," does not include wages, hours, and working conditions, to reiterate employee rights about discussing terms and conditions of employment and reporting to governmental agencies, and to make clear that prohibitions against "conflicting outside interests" do not cover forming or joining (or refraining from joining) labor organizations of an employee's choice and **WE HAVE** informed employees of these clarifications.

WE HAVE rescinded the aspects of Business Conduct and Global Compliance FAQ regarding Confidential Information described above and revised it to conform with the definition of Apple Confidential Information described above and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the aspects of the Business Conduct Policy described above and revised it to make clear that Apple Confidential Information does not include wages, hours, and working conditions, that employees may communicate about labor disputes, to clarify that employees may not respond to public inquiries or participate in speaking engagements where employees could be construed as speaking on behalf of Apple, to clarify that employees may publish articles but must receive approval about articles about Apple products or services or could be seen as a conflict of interest, make clear that a conflict of interest does not include forming, joining, or assisting a union, or engaging in protected, concerted activity, to make clear that employees do not need to notify a manager of outside employment that complies with our policy, and to inform employees that searches will not be used to monitor employees' protected, concerted activity, and **WE HAVE** informed employees of these revisions.

The National Labor Relations Board is an independent Federal agency created in 1935 to enforce the National Labor Relations Act. We conduct secret-ballot elections to determine whether employees want union representation and we investigate and remedy unfair labor practices by employers and unions. To find out more about your rights under the Act and how to file a charge or election petition, you may speak confidentially to any agent with the Board's Regional Office set forth below or you may call the Board's toll-free number 1-844-762-NLRB (1-844-762-6572). Hearing impaired callers who wish to speak to an Agency representative should contact the Federal Relay Service (link is external) by visiting its website at https://www.federalrelay.us/tty (link is external), calling one of its toll free numbers and asking its Communications Assistant to call our toll free number at 1-844-762-NLRB.

THIS IS AN OFFICIAL NOTICE AND MUST NOT BE DEFACED BY ANYONE.

THIS NOTICE MUST REMAIN POSTED FOR 60 CONSECUTIVE DAYS FROM THE DATE OF POSTING AND MUST NOT BE ALTERED DEFACED OR COVERED BY ANY OTHER MATERIAL. ANY QUESTIONS CONCERNING THIS NOTICE OR COMPLIANCE WITH ITS PROVISIONS MAY BE DIRECTED TO, THE ASSISTANT TO THE REGIONAL DIRECTOR NATHAN SEIDMAN AT nathan.seidman@nlrb.gov or (213) 634-6518.

32-CA-284428

FORM NLRB-4722

NOTICE TO EMPLOYEES

POSTED PURSUANT TO A SETTLEMENT AGREEMENT APPROVED BY A REGIONAL DIRECTOR OF THE NATIONAL LABOR RELATIONS BOARD

AN AGENCY OF THE UNITED STATES GOVERNMENT

THE NATIONAL LABOR RELATIONS ACT GIVES YOU THE RIGHT TO:

- Form, join, or assist a union;
- Choose a representative to bargain with your employer on your behalf;
- Act together with other employees for your benefit and protection;
- Choose not to engage in any of these protected activities.

WE HAVE rescinded the aspects of the Workplace Searches and Privacy Policy described above and revised it to conform with the definition of Apple Confidential Information described above and to inform employees that searches will not be used to monitor employees' protected, concerted activity and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the aspects of the Misconduct and Discipline Policy described above and revised it to conform with the definition of Apple Confidential Information described above, to reiterate employee rights under the National Labor Relations Act relating to certain workplace investigations relating to alleged unfair labor practices under the National Labor Relations Act, to clarify when recording and photography is permitted and prohibited, and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the aspects of the Social Media and Online Communications Policy described above and revised it to conform with the definition of Apple Confidential Information described above and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the prior version of the Confidentiality Obligations Upon Termination of Employment statement, which contained an overbroad definition of proprietary information, and revised it to conform with the definition of Apple Confidential Information described above and **WE HAVE** informed employees of these revisions.

WE WILL NOT in any like or related manner interfere with your rights under Section 7 of the Act.

APPLE INC.

_____
(Charged Party)

Dated: _____ **By:** _____
(Representative) (Title)

The National Labor Relations Board is an independent Federal agency created in 1935 to enforce the National Labor Relations Act. We conduct secret-ballot elections to determine whether employees want union representation and we investigate and remedy unfair labor practices by employers and unions. To find out more about your rights under the Act and how to file a charge or election petition, you may speak confidentially to any agent with the Board's Regional Office set forth below or you may call the Board's toll-free number 1-844-762-NLRB (1-844-762-6572). Hearing impaired callers who wish to speak to an Agency representative should contact the Federal Relay Service (link is external) by visiting its website at https://www.federalrelay.us/tty (link is external), calling one of its toll free numbers and asking its Communications Assistant to call our toll free number at 1-844-762-NLRB.

THIS IS AN OFFICIAL NOTICE AND MUST NOT BE DEFACED BY ANYONE.

THIS NOTICE MUST REMAIN POSTED FOR 60 CONSECUTIVE DAYS FROM THE DATE OF POSTING AND MUST NOT BE ALTERED DEFACED OR COVERED BY ANY OTHER MATERIAL. ANY QUESTIONS CONCERNING THIS NOTICE OR COMPLIANCE WITH ITS PROVISIONS MAY BE DIRECTED TO, THE ASSISTANT TO THE REGIONAL DIRECTOR NATHAN SEIDMAN AT nathan.seidman@nlrb.gov or (213) 634-6518.

UNITED STATES GOVERNMENT
NATIONAL LABOR RELATIONS BOARD
SETTLEMENT AGREEMENT

IN THE MATTER OF

APPLE INC. **Case 32-CA-284428**

Subject to the approval of the Regional Director for the National Labor Relations Board, the Charged Party Apple Inc. and the Charging Party Ashley Marie Gjovik

HEREBY AGREE TO SETTLE THE ABOVE MATTER AS FOLLOWS:

POSTING OF NOTICE TO EMPLOYEES — The Charged Party will post a link to a copy of the Notice in English and in additional languages if the Regional Director decides that it is appropriate to do so, on the Policies and Notices page of its People intranet and keep such link continuously posted there for 60 consecutive days from the date it was originally posted. Such link will read, "This Notice is Posted Pursuant to a Settlement Agreement Approved by the Regional Director of Region 21 of the National Labor Relations Board in Case 32-CA-284428." Charged Party will also post, on a public-facing website maintained indefinitely by Charged Party containing legal notices, an explanation of revisions to the definition of Confidential Information (or comparable term) in the Confidentiality and Intellectual Property Agreement. To document its compliance with this requirement, the Charged Party will submit screen shots of the posting to include screen shots of the path to the intranet page that shows the Notice, along with a fully completed Certification of Posting form, via the Agency's e-filing portal at www.nlrb.gov. Should further investigation or verification of the intranet or website posting become necessary, the Charged Party will provide appropriate intranet or website access to the Compliance Assistant or Compliance Officer assigned to the case(s).

COMPLIANCE WITH NOTICE — The Charged Party will comply with all the terms and provisions of said Notice**.**

NON-ADMISSION—By entering into this Agreement the Charged Party does not admit to any violation of the National Labor Relations Act ("Act").

ADDITIONAL TERMS – The Charged Party agrees that it will not enforce the definition of Proprietary Information (or similar terms) set forth in any version of the Confidentiality and Intellectual Property Agreement ("IPA") effective as of the date that this Agreement is executed to the extent that such definition covers terms and conditions of employment protected under Section 7 of the Act.

A further material term of this Agreement is that the Charged Party is directed to prospectively clarify the definition of Proprietary Information (or similar terms) in the IPA and make other clarifications to the IPA relating to the Section 7 rights of employees or at its option issue a new IPA for certain employees with prospective effect, with such clarified definition of Proprietary

Information (or similar terms) or such new agreement as reflected in the attached Appendix A, and has agreed to revise certain other policies, as reflected in the attached Appendix B.[1]

SCOPE OF THE AGREEMENT — This Agreement settles only the allegations in the above-captioned case(s), including all allegations covered by the attached Notice to Employees made part of this agreement, and does not settle any other case(s) or matters, including, but not limited to, 32-CA-282142, 32-CA-283161, and 32-CA-284441. It does not prevent persons from filing charges, the General Counsel from prosecuting complaints, or the Board and the courts from finding violations with respect to matters that happened before this Agreement was approved regardless of whether General Counsel knew of those matters or could have easily found them out. The General Counsel reserves the right to use the evidence obtained in the investigation and prosecution of the above-captioned case(s) for any relevant purpose in the litigation of this or any other case(s), and a judge, the Board and the courts may make findings of fact and/or conclusions of law with respect to said evidence.

PARTIES TO THE AGREEMENT — If the Charging Party fails or refuses to become a party to this Agreement and the Regional Director determines that it will promote the policies of the National Labor Relations Act, the Regional Director may approve the settlement agreement and decline to issue or reissue a Complaint in this matter. If that occurs, this Agreement shall be between the Charged Party and the undersigned Regional Director. In that case, a Charging Party may request review of the decision to approve the Agreement. If the General Counsel does not sustain the Regional Director's approval, this Agreement shall be null and void.

AUTHORIZATION TO PROVIDE COMPLIANCE INFORMATION AND NOTICES DIRECTLY TO CHARGED PARTY — Counsel for the Charged Party authorizes the Regional Office to forward the cover letter describing the general expectations and instructions to achieve compliance, a conformed settlement, original notices and a certification of posting directly to the Charged Party. If such authorization is granted, Counsel will be simultaneously served with a courtesy copy of these documents.

Yes _____ Initials No MLS Initials

PERFORMANCE — Performance by the Charged Party with the terms and provisions of this Agreement shall commence immediately after the Agreement is approved by the Regional Director, or if the Charging Party does not enter into this Agreement, performance shall commence immediately upon receipt by the Charged Party of notice that no review has been requested or that the General Counsel has sustained the Regional Director. The Charged Party agrees that in case of non-compliance with any of the terms of this Settlement Agreement by the Charged Party, and after 14 days notice from the Regional Director of the National Labor Relations Board of such non-compliance without remedy by the Charged Party, the Regional Director will reissue the complaint previously issued on October 3, 2024, in the instant case. Thereafter, the General Counsel may file a motion for default judgment with the Board on the

[1] Charged Party, through counsel, will provide Charging Party with notice of these revisions.

allegations of the complaint. The Charged Party understands and agrees that the allegations of the aforementioned complaint will be deemed admitted and its Answer to such complaint will be considered withdrawn. The only issue that may be raised before the Board is whether the Charged Party defaulted on the terms of this Settlement Agreement. The Board may then, without necessity of trial or any other proceeding, find all allegations of the complaint to be true and make findings of fact and conclusions of law consistent with those allegations adverse to the Charged Party on all issues raised by the pleadings. The Board may then issue an order providing a full remedy for the violations found as is appropriate to remedy such violations. The parties further agree that a U.S. Court of Appeals Judgment may be entered enforcing the Board order ex parte, after service or attempted service upon Charged Party/Respondent at the last address provided to the General Counsel.

NOTIFICATION OF COMPLIANCE — Each party to this Agreement will notify the Regional Director in writing what steps the Charged Party has taken to comply with the Agreement. This notification shall be given within 5 days, and again after 60 days, from the date of the approval of this Agreement. If the Charging Party does not enter into this Agreement, initial notice shall be given within 5 days after notification from the Regional Director that the Charging Party did not request review or that the General Counsel sustained the Regional Director's approval of this agreement. No further action shall be taken in the above captioned case(s) provided that the Charged Party complies with the terms and conditions of this Settlement Agreement and Notice.

Charged Party Apple Inc.	**Charging Party Ashley Marie Gjovik**
By: Name and Title Date /s/ Mark L. Stolzenburg March 25, 2025 Print Name and Title below Attorney for Apple Inc.	By: Name and Title Date Ashley M. Gjovik April 3 2025 Print Name and Title below **Ashley M. Gjovik, Charging Party**
Recommended By: Date ELVIRA PEREDA Counsel for the Acting General Counsel	Approved By: Date NATHAN M. SEIDMAN Acting Regional Director, Region 21

Charged Party Initials: MLS Charging Party Initials: AMG

(To be printed and posted on official Board notice form)

THE NATIONAL LABOR RELATIONS ACT GIVES YOU THE RIGHT TO:

- Form, join, or assist a union;
- Choose a representative to bargain with us on your behalf;
- Act together with other employees for your benefit and protection;
- Choose not to engage in any of these protected activities.

WE WILL NOT interfere with, restrain, or coerce you in the exercise of the above rights.

YOU HAVE THE RIGHT to discuss wages, hours and working conditions and **WE WILL NOT** do anything to interfere with your exercise of that right.

WE WILL NOT promulgate, maintain, or enforce any rule that defines confidential information as "anything not explicitly, publicly, or purposefully disclosed by Apple."

WE WILL NOT promulgate, maintain, or enforce a Confidentiality and Intellectual Property Agreement, Business Conduct Policy, Misconduct and Discipline Policy, Social Media and Online Communications Policy, Confidentiality Obligations Upon Termination of Employment statement, or a Business Conduct and Global Compliance FAQ regarding confidential information that broadly defines "confidential" or "proprietary" information, or relies upon any other overly broad definitions of those terms, without contemporaneously notifying employees of their rights to discuss wages, hours, or working conditions and their rights to engage in union or other protected, concerted activity under the NLRA.

WE WILL NOT promulgate, maintain, or enforce a Business Conduct Policy that broadly restricts public speaking, responses to press inquiries and publishing articles without contemporaneously notifying employees of their rights to speak publicly, respond to press inquiries and publish articles regarding their wages, hours, or working conditions, or their union or other protected, concerted activity under the NLRA.

WE WILL NOT promulgate, maintain, or enforce a Business Conduct Policy that broadly restricts "conflicts of interest" or "outside activities," without contemporaneously notifying employees that such policies do not restrict their right to form, join or assist a union, or engage in other protected, concerted activity and that these activities are not considered to be conflicts of interest or outside activities under such policy.

WE WILL NOT promulgate, maintain, or enforce a Business Conduct Policy that broadly prohibits sharing of employee personal identifying information if such policy could be interpreted as prohibiting the sharing of personal contact information, employment history, compensation or other terms and conditions of employment.

WE WILL NOT promulgate, maintain, or enforce a Workplace Searches and Privacy Policy that advises you that we have the right to access Apple's network or systems, or any non-Apple

device used to conduct Apple business, without contemporaneously advising you that we will not exercise our right of access to monitor your union or other protected, concerted activity.

WE WILL NOT promulgate, maintain, or enforce a Misconduct and Discipline Policy that fails to reiterate employee rights during investigations that Apple may conduct regarding alleged unfair labor practices under the National Labor Relations Act, and/or contains overly broad restrictions on photography and recording.

WE WILL NOT advise you that you are subject to discipline for violating overly broad rules regarding confidential or proprietary information or for failing to report alleged violations of overly broad rules relating to confidential or proprietary information.

WE WILL NOT advise you that you are subject to discipline for violating overly broad rules regarding photographing, video or audio recording that prohibit the recording of protected, concerted activity.

WE HAVE clarified the aspects of the Confidentiality and Intellectual Property Agreement described above and revised it to make clear that the definition of "Proprietary Information," which was changed to "Apple Confidential Information," does not include wages, hours, and working conditions, to reiterate employee rights about discussing terms and conditions of employment and reporting to governmental agencies, and to make clear that prohibitions against "conflicting outside interests" do not cover forming or joining (or refraining from joining) labor organizations of an employee's choice and **WE HAVE** informed employees of these clarifications.

WE HAVE rescinded the aspects of Business Conduct and Global Compliance FAQ regarding Confidential Information described above and revised it to conform with the definition of Apple Confidential Information described above and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the aspects of the Business Conduct Policy described above and revised it to make clear that Apple Confidential Information does not include wages, hours, and working conditions, that employees may communicate about labor disputes, to clarify that employees may not respond to public inquiries or participate in speaking engagements where employees could be construed as speaking on behalf of Apple, to clarify that employees may publish articles but must receive approval about articles about Apple products or services or could be seen as a conflict of interest, make clear that a conflict of interest does not include forming, joining, or assisting a union, or engaging in protected, concerted activity, to make clear that employees do not need to notify a manager of outside employment that complies with our policy, and to inform employees that searches will not be used to monitor employees' protected, concerted activity, and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the aspects of the Workplace Searches and Privacy Policy described above and revised it to conform with the definition of Apple Confidential Information described above and to inform employees that searches will not be used to monitor employees' protected, concerted activity and **WE HAVE** informed employees of these revisions.

Charged Party Initials: MLS Charging Party Initials: AMG

WE HAVE rescinded the aspects of the Misconduct and Discipline Policy described above and revised it to conform with the definition of Apple Confidential Information described above, to reiterate employee rights under the National Labor Relations Act relating to certain workplace investigations relating to alleged unfair labor practices under the National Labor Relations Act, to clarify when recording and photography is permitted and prohibited, and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the aspects of the Social Media and Online Communications Policy described above and revised it to conform with the definition of Apple Confidential Information described above and **WE HAVE** informed employees of these revisions.

WE HAVE rescinded the prior version of the Confidentiality Obligations Upon Termination of Employment statement, which contained an overbroad definition of proprietary information, and revised it to conform with the definition of Apple Confidential Information described above and **WE HAVE** informed employees of these revisions.

WE WILL NOT in any like or related manner interfere with your rights under Section 7 of the Act.

APPLE INC.
(Charged Party)

Dated: _____ **By:** _____
(Representative) (Title)

The National Labor Relations Board is an independent Federal agency created in 1935 to enforce the National Labor Relations Act. We conduct secret-ballot elections to determine whether employees want union representation and we investigate and remedy unfair labor practices by employers and unions. To find out more about your rights under the Act and how to file a charge or election petition, you may speak confidentially to any agent with the Board's Regional Office set forth below or you may call the Board's toll-free number 1-844-762-NLRB (1-844-762-6572). Callers who are deaf or hard of hearing who wish to speak to an NLRB representative should send an email to relay.service@nlrb.gov. An NLRB representative will email the requestor with instructions on how to schedule a relay service call.

US Court House, Spring Street
312 N Spring Street, 10th Floor
Los Angeles, CA 90012

Telephone: (213)894-5200
Hours of Operation: 8:30 a.m. to 5 p.m.

THIS IS AN OFFICIAL NOTICE AND MUST NOT BE DEFACED BY ANYONE

This notice must remain posted for 60 consecutive days from the date of posting and must not be altered, defaced or covered by any other material. Any questions concerning this notice or compliance with its provisions may be directed to the above Regional Office's Compliance Officer.

Charged Party Initials: MLS _____ Charging Party Initials: AMG _____

O. EXHIBIT O: NIH

Exhibit: OHRP Complaint No. 00709517

Reporting an Incident to OHRP: Trial ID NCT04196595 (Apple Women's Health Study)

From Ashley Gjovik <ashleymgjovik@protonmail.com>

To OHRP-DCO@hhs.gov

CC AppleWomensHealthStudy@hsph.harvard.edu, jukica@niehs.nih.gov, baird@niehs.nih.gov

Date Wednesday, March 11th, 2026 at 2:05 AM

OHRP Incident Report

Incident Type: Serious Non-Compliance / Unanticipated Problem Involving Risks to Subjects
Regulatory Framework: 45 CFR Part 46 (Common Rule); 42 U.S.C. § 282(j)
Reported by: Ex-employee of Sponsor / Responsible Party

Study Title: Apple Women's Health Study
Trial ID: NCT04196595
Principal Investigator / Conducting Institution: Harvard T.H. Chan School of Public Health
Sponsor / Responsible Party: Apple Inc.
Additional Federal Partner: National Institute of Environmental Health Sciences (NIEHS)
Trial Registration Date: 2019 (ongoing as of 2026)
Stated Study Goals: (1) Identify Menstrual Cycle Patterns; (2) Epidemiologic Description of Menstrual Cycle; (3) Determine prevalence of gynecologic health conditions

Hello,

This complaint concerns the Apple Women's Health Study (AWHS), a clinical trial registered on ClinicalTrials.gov (NCT04196595 (https://clinicaltrials.gov/study/NCT04196595)) since 2019 and currently ongoing. The trial is sponsored by Apple Inc. and conducted by Harvard T.H. Chan School of Public Health, in partnership with NIEHS as part of what has been described as a major long-term study of women's health. Medscape reported the study in 2023 as "a 10-year project among Harvard, Apple, and the National Institute of Environmental Health Sciences (NIEHS) that is unprecedented in size and scope." (Medscape, 2023 (https://www.medscape.com/s/viewarticle/996078?form=fpf)) The subject matter involves collection of highly sensitive and intimate reproductive health data, specifically related to ovulation and menstruation. The ClinicalTrials page lists the top study goals as "Identify Menstrual Cycle Patterns" and "Epidemiologic Description of Menstrual Cycle" with a secondary goal of "Determine prevalence of gynecologic health conditions."

The subject matter of the trial involves ovulation and menstruation — intimate reproductive health data of a highly personal nature. The corporate sponsor has actively recruited its own employees as research subjects to increase enrollment numbers since at least 2019. This practice creates a structural and inescapable conflict of interest: employees being asked to participate by or through their employer (who is simultaneously the trial's sponsor) face an inherent power imbalance in which declining to participate may reasonably be perceived as carrying professional consequences. The team's own reports indicate that as of 2023, when the overall participation was around one hundred thousand, that only two states provided more than ten thousand participants -- California and Texas -- where

the corporation's headquarters are located. In fact, California is the only state indicated to be well above ten thousand indicating it may even account for over 80% of the participants -- with a large amount originating from its corporate offices or the family members of its corporate employees. (Overall participant enrollment by state, https://hsph.harvard.edu/research/apple-womens-health-study/study-updates/2023-apple-womens-health-study-newsletter-four-years-in-review/).

Overall, the team's conduct raises serious compliance concerns under:

- 45 CFR 46.116(b)(2): Informed consent must be free from coercion or undue influence. Employer-to-employee recruitment by the sponsoring corporation constitutes a paradigmatic example of undue influence, as employees cannot freely decline without fear of workplace consequences.
- 45 CFR 46.111(a)(3) and 46.111(b): The IRB is required to ensure equitable subject selection and to apply additional protections when subjects are vulnerable to coercion. Employees of a trial's corporate sponsor constitute a vulnerable population in precisely the sense these provisions are designed to address. The IRB either approved this recruitment pathway without adequate safeguards, or the recruitment occurred without IRB knowledge — both of which are reportable failures.

This study/trial has been registered and operating since 2019. The recruitment of employees by the corporate sponsor appears to be a sustained and ongoing recruitment strategy, not an isolated incident. This constitutes continuing non-compliance within the meaning of 45 CFR Part 46. The IRB's apparent failure to identify or correct this practice over a multi-year period is itself a significant matter of concern warranting investigation.

This complaint concerns Apple Inc.'s response to a non-enrolled individual — a former Apple employee who declined enrollment and subsequently spoke publicly about the coercive nature of the study's recruitment practices and raised questions about the integrity of the trial's enrollment and consent process. In response, Apple Inc. has pursued legal action in federal court against that individual. In the matter of *Ashley Gjovik v. Apple Inc.*, Case No. 3:23-cv-04597-EMC (N.D. Cal.), Apple has taken the position that the employee's testimony, speech, and complaints about the corporation's recruitment practices are confidential, and has sought sealing orders, compelled deletion of public criticism, prior restraint gag orders, and sanctions against the individual for filing complaints with government agencies and speaking publicly about concerns that Apple's recruitment of employees into a highly personal medical study is unethical, improper, and likely unlawful and that Apple was trying to designate her complaints as "confidential". (See *Ashley Gjovik v Apple Inc,* 3:23-cv-04597-EMC, Northern District of California, https://www.courtlistener.com/docket/67772913/gjovik-v-apple-inc/?filed_after=&filed_before=&entry_gte=&entry_lte=&order_by=desc).

The specific nature of the data at issue warrants particular attention. Apple's own litigation filings reveal that the study's scope as implemented includes monitoring of employee cervical mucus and vaginal secretions, and at the same time Apple also sought to register employees' sex partners and require those sex partners to execute non-disclosure agreements for a separate "study". I complained about both of these things -- while I worked at Apple and after. My deposition testimony at issue was simply summarizing my prior complaints about Apple's recruitment practices for this and other studies. Apple then further claimed in that litigation that employee complaints about being asked to submit to this type of study and monitoring are themselves confidential like trade secrets, and is currently seeking a gag order prohibiting employees from discussing any of it. The IRB's privacy assessment under 45 CFR 46.111(a)(7) must be evaluated against this specific reality — not merely the abstract description of a menstrual health study, but an employer asserting proprietary control over employees' reproductive and sexual data, the identities of their sexual partners, and the complaints those employees made about being subjected to it.

In making this complaint to you right now and when I attach a copy in my court filings for this matter, Apple will claim the content in this email is confidential and proprietary, should be sealed, and I should be sanctioned for continuing to violate court "rules" (where the corporation is abusing a protective order to apply to existing complaints and to use as a private prior restraint against employees and critics about its operations). This secrecy includes, and is targeted to conceal, how Apple runs recruitment for clinical trials including ones that are done as a formal partnership with the government (like here, with NIEHS). An employer recruiting its own employees to disclose intimate reproductive health information as research subjects raises acute privacy concerns that the IRB was required to specifically address under 45 CFR 46.111(a)(7) (The IRB must ensure adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data). When the entity collecting this data is also the subject's employer, the adequacy of any privacy protections is inherently compromised. Employees have reasonable cause to fear that reproductive health information disclosed in a sponsor-controlled study may not remain segregated from their employment relationship.

Apple's position, as stated in that litigation including attached filings, is that it is impermissible for the complainant to raise these concerns publicly, to communicate them to third parties, or to submit this very complaint to OHRP. Apple appears to be mis-using a legal processes as a private prior restraint mechanism against employees and critics discussing how the corporation operates clinical trials conducted in formal partnership with the federal government. This raises a question about how often Apple engages in this kind of conduct and how else it's obstructed complaints about this study.

Further, Apple's conduct implicates a number of issues in the clinical trial and human research regulatory framework:

- **42 U.S.C. § 282(j):** Clinical trial registration exists precisely because human subjects research is subject to public accountability. Apple Inc. cannot simultaneously hold a registered trial out as a public research enterprise — particularly one conducted in federal partnership with NIEHS — and seek court orders suppressing public speech about how that trial recruits its subjects.
- **45 CFR 46.116(b)(8):** Informed consent must identify whom subjects may contact with questions or concerns about the research and their rights. This provision reflects the regulatory framework's treatment of the ability to raise concerns as an intrinsic right — not a privilege the sponsor may litigate away through injunctive relief.
- **Chilling Effect on Current and Future Subjects:** By pursuing legal action against a person who declined to enroll and raised compliance concerns, Apple has sent a direct signal to every current and potential subject that raising concerns about this trial carries severe legal consequences. This compounds the coercive environment described above and further undermines the voluntariness of any consent obtained from employees in this environment.
- **Sponsor's Posture Toward Compliance:** The decision to pursue legal suppression of scrutiny — rather than address the underlying recruitment concerns — is directly relevant to OHRP's assessment of whether Apple Inc. can be trusted to operate a compliant human subjects research program. It reflects an institutional posture that treats public accountability as a threat to be neutralized rather than an obligation to be met.

The complainant respectfully requests that OHRP:

- Investigate the IRB's review and approval of the employee recruitment pathway, and assess whether adequate protections against undue influence were required and implemented.
- Assess whether consent processes conducted under this coercive recruitment environment meet the voluntariness requirements of 45 CFR 46.116.

- Determine how many participants in the total participants for this study are Apple employees or direct family members of Apple employees, and determine what % of the total population of the study makes the study population impermissibly dominant with employees.
- Evaluate whether the IRB's privacy provisions under 45 CFR 46.111(a)(7) adequately address the risks created by a corporate employer-sponsor collecting reproductive health data from its own employees.
- Consider Apple Inc.'s litigation conduct in *Gjovik v. Apple Inc.,* No. 3:23-cv-04597-EMC (N.D. Cal.), as evidence bearing on the sponsor's compliance posture and the integrity of the trial's ongoing operations.
- Inquire whether other complaints or concerns about this study have been similarly suppressed by Apple through any type of conduct, including litigation "protective orders"
- Determine whether suspension or additional oversight of the trial is warranted pending investigation.

The following documents are submitted in support of this complaint or are available upon request:

- ClinicalTrials.gov registration record (https://clinicaltrials.gov/study/NCT04196595)
- Documentation of legal action and threatened speech restraints and other injunctive relief against complainant (*Ashley Gjovik v Apple Inc,* 3:23-cv-04597-EMC, Northern District of California)
- AWHS 2023 Four Years in Review Newsletter (participant enrollment by state): HSPH.edu (https://hsph.harvard.edu/research/apple-womens-health-study/study-updates/2023-apple-womens-health-study-newsletter-four-years-in-review/)
- Medscape coverage of AWHS scope: Medscape, 2023 (https://www.medscape.com/s/viewarticle/996078?form=fpf)
- March 14 2023 Telerama magazine article (translated from French to English) where I and my coworkers criticized Apple's use of employee data for this specific study.

Note: I contacted the Study's contact list at Harvard (cc'd here) on March 8th, asking for a response on these matters but received no response by March 10th. I told them if I didn't receive a response I'd file by end of day, and no response was provided so now I'm filing that complaint.

This complaint is submitted in good faith based on direct knowledge of the events described. The complainant is aware that Apple Inc. may contend that the submission of this complaint itself violates litigation-related orders or confidentiality designations. The complainant submits that the filing of a good-faith regulatory complaint with a federal oversight body is protected activity and that any such contention by Apple would itself constitute further evidence of the sponsor's attempt to suppress oversight of a federally registered human subjects research study. The complainant understands that OHRP may contact the submitter for additional information.

Ashley Gjovik, B.S., PMP, J.D.
Dated: March 11 2026
San Jose, California
Ex-Apple Employee (2015-2021)

18.56 MB 5 files attached

APPLE WOMENS HEALTH STUDY LITIGATION PORTFOLIO.pdf 17.16 MB

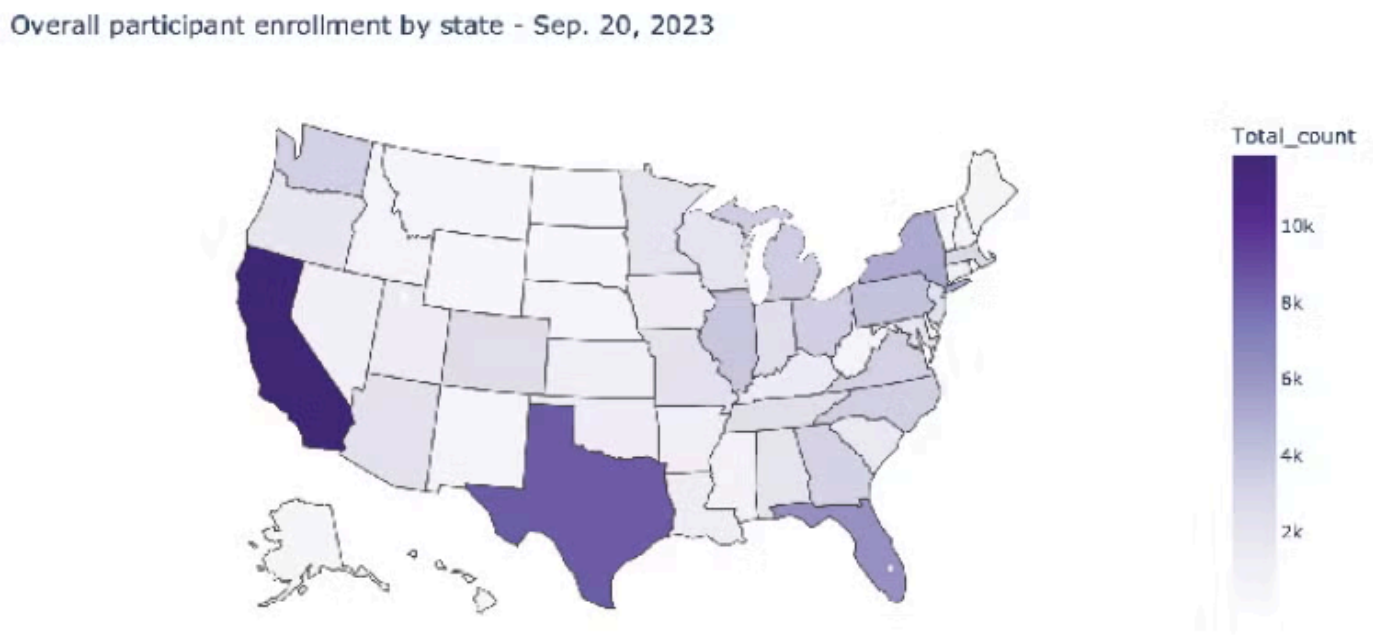
Study Details _ NCT04196595 _ Apple Women's Health Study _ ClinicalTrials.gov.pdf 638.43 KB

NIH partners with Apple and Harvard University on Women's Health Study _ National Institutes of Health (NIH).pdf
153.50 KB

Locations 2023 Apple Women's Health Study newsletter_ four years in review _ Study Updates _ Harvard T.H...th.pdf
209.68 KB

Ashley Gjøvik, lanceuse d'alerte licenciée par Apple, seule contre tous - en-US.pdf 436.57 KB

allows for investigating the impact of environmental factors on a person's menstrual cycles and health. Participant experiences reflect the wide range of geographic, cultural, social, and economic factors that may help AWHS better understand menstrual health.



The map shows how many participants in AWHS enrolled from the US States. The darker the color, the higher the number as shown on the scale. The relative color difference also shows what percentage of our total cohort comes from each state, so darker colored states contribute a higher percentage of the cohort. CA, FL, and TX are so high in percentage since their populations also comprise a similar percentage of the overall US population.

While each menstrual journey is unique, many often share similar experiences throughout such as menstrual symptoms and menstrual hygiene.

National Institutes of Health
Turning Discovery Into Health

Tuesday, September 10, 2019

NIH partners with Apple and Harvard University on Women's Health Study

The National Institutes of Health, Apple, and the Harvard T. H. Chan School of Public Health announced their research partnership for a major long-term study of women's health. The collaboration will permit researchers to study conditions including pregnancy, infertility, polycystic ovary syndrome (PCOS), menopausal transition, and osteoporosis. Apple's new Research App will help users participate in the study and will be a free download in the App Store later this year.

The intention is to improve women's health by identifying the factors that impact women from around the country. This new study will connect academic medical institutions, healthcare organizations, and Apple products with the goal of contributing to medical science and helping to create the next generation of innovative health software.

The National Institute of Environmental Health Sciences (NIEHS), the NIH institute involved in the partnership, has several of the world's leading scientists on women's health and population studies. NIEHS will provide expert advice and data analysis for the Apple Women's Health Study.

"This is an exciting opportunity for NIEHS researchers to contribute to the study design and use the resulting data to answer novel questions, not only important to women of reproductive age, but to women of all ages," said Dale Sandler, Ph.D., chief of the NIEHS Epidemiology Branch.

Allen Wilcox, M.D., Ph.D., Scientist Emeritus at NIEHS, has spent 40 years studying fertility and pregnancy, and welcomes this opportunity to work with Apple and colleagues at Harvard. He is optimistic about the medical advances that could come from this collaboration.

"Studies conducted with commercial cycle and fertility tracking apps have great potential for making important contributions to science, because they can enroll much larger samples of women and from far more diverse backgrounds," added Wilcox. "We want to do our part to make this new method of data collection a scientifically valid source of health information."

About the National Institute of Environmental Health Sciences (NIEHS): NIEHS supports research to understand the effects of the environment on human health and is part of the National Institutes of Health. For more information on NIEHS or environmental health topics, visit www.niehs.nih.gov or subscribe to a news list.

About the National Institutes of Health (NIH): NIH, the nation's medical research agency, includes 27 Institutes and Centers and is a component of the U.S. Department of Health and Human Services. NIH is the primary federal agency conducting and supporting basic, clinical, and translational medical research, and is investigating the causes, treatments, and cures for both common and rare diseases. For more information about NIH and its programs, visit www.nih.gov.

NIH…Turning Discovery Into Health®

Institute/Center

National Institute of Environmental Health Sciences (NIEHS)

Contact

Robin Arnette
919-541-5143

Connect with Us

Subscribe to news releases
RSS Feed

National Institutes of Health

9000 Rockville Pike
Bethesda, Maryland 20892

NIH…Turning Discovery Into Health®

Follow Us

Glossary

Glossary

ClinicalTrials.gov

National Library of Medicine
National Center for Biotechnology Information

The U.S. government does not review or approve the safety and science of all studies listed on this website.

Read our full disclaimer (https://clinicaltrials.gov/about-site/disclaimer) for details.

Recruiting

Apple Women's Health Study

ClinicalTrials.gov ID NCT04196595

Sponsor Apple Inc.

Information provided by Apple Inc. (Responsible Party)

Last Update Posted 2024-07-03

Study Details Tab

Study Overview

Brief Summary

This is an observational longitudinal study to advance the understanding of menstrual cycle and gynecologic health conditions including PCOS, infertility and breast cancer.The study will be hosted within the Research app(available on App Store), which allows a user to find, enroll, and participate in Apple-supported health-related research studies.

Official Title

Apple Women's Health Study

Conditions

Menstrual Cycle | Ovulation | Menstruation | Polycystic Ovary Syndrome | Infertility | Menopause | Reproduction | Reproductive Health

Other Study ID Numbers

- Pro00037562

Study Start (Actual)

2019-11-14

Primary Completion (Estimated)

2029-11

Study Completion (Estimated)

2029-11

Enrollment (Estimated)

500000

Study Type

Observational

Resource links provided by the National Library of Medicine

MedlinePlus Genetics (https://medlineplus.gov/genetics/) related topics: Polycystic ovary syndrome (https://medlineplus.gov/genetics/condition/polycystic-ovary-syndrome)

MedlinePlus (https://medlineplus.gov/) related topics: Infertility (https://medlineplus.gov/infertility.html) Polycystic Ovary Syndrome (https://medlineplus.gov/polycysticovarysyndrome.html)

FDA Drug and Device Resources (https://clinicaltrials.gov/fda-links)

Contacts and Locations

This section provides contact details for people who can answer questions about joining this study, and information on where this study is taking place.

To learn more, please see the Contacts and Locations section in How to Read a Study Record (https://clinicaltrials.gov/study-basics/how-to-read-study-record#contacts-and-locations).

Study Contact

Name: Shruthi Mahalingaiah, MD
Phone Number: 617-432-1356
Email: AppleWomensHealthStudy@hsph.harvard.edu

This study has 1 location

United States

Massachusetts Locations

Boston, Massachusetts, United States, 02115
Recruiting
Harvard T.H. Chan School of Public Health
Contact : Shruthi Mahalingaiah
617-432-1356
AppleWomensHealthStudy@hsph.harvard.edu

Participation Criteria

Researchers look for people who fit a certain description, called eligibility criteria. Some examples of these criteria are a person's general health condition or prior treatments.

For general information about clinical research, read Learn About Studies (https://clinicaltrials.gov/study-basics/learn-about-studies).

Eligibility Criteria

Description

Inclusion Criteria:

- Have menstruated at least once
- Be at least 18 years old (at least 19 years old in Alabama and Nebraska, at least 21 years old in Puerto Rico)
- Live in the United States of America
- Be comfortable communicating in written and spoken English
- Have installed the Apple Research app on your iPhone
- Not share your iCloud account or iPhone with anyone else
- Be willing and able to provide informed consent to participate in the study

Study Population

Convenience sampling of individuals who have ever menstruated and meet other eligibility criteria

Ages Eligible for Study

18 Years and older (Adult, Older Adult)

Sexes Eligible for Study

All

Accepts Healthy Volunteers

Yes

Sampling Method

Non-Probability Sample

Study Plan

This section provides details of the study plan, including how the study is designed and what the study is measuring.

How is the study designed?

Design Details

Observational Model : Cohort
Time Perspective: Prospective

What is the study measuring?

Primary Outcome Measures

Outcome Measure	Measure Description	Time Frame
Identify Menstrual Cycle Patterns	Characterized using duration of menstrual flow, and cycle length in unit of days.	Up to 10 years
Epidemiologic Description of Menstrual Cycle	Characterized using cycle patterns and self-reported demographics, no unit of measure	Up to 10 years

Secondary Outcome Measures

Outcome Measure	Measure Description	Time Frame
Determine prevalence of gynecologic health conditions	Characterized using menstrual cycle patterns and self-reported health conditions, no unit of measure	Up to 10 years

Collaborators and Investigators

This is where you will find people and organizations involved with this study.

Sponsor

Apple Inc.

Collaborators

- Harvard School of Public Health (HSPH)
- National Institute of Environmental Health Sciences (NIEHS)

Investigators

- Principal Investigator: Michelle A Williams, SM, ScD, Harvard School of Public Health (HSPH)
- Principal Investigator: Russ B Hauser, MD, MPH, ScD, Harvard School of Public Health (HSPH)
- Principal Investigator: Brent A Coull, PhD, Harvard School of Public Health (HSPH)
- Principal Investigator: Shruthi Mahalingaiah, MD, MS, Harvard School of Public Health (HSPH)

Publications

From PubMed

These publications are automatically filled in from PubMed, a public database of scientific and medical articles, and may or may not be about the study.

- Zhang CY, Li H, Zhang S, Suharwardy S, Chaturvedi U, Fischer-Colbrie T, Maratta LA, Onnela JP, Coull BA, Hauser R, Williams MA, Baird DD, Jukic AMZ, Mahalingaiah S, Curry CL. Abnormal uterine bleeding patterns determined through menstrual tracking among participants in the Apple Women's Health Study. Am J Obstet Gynecol. 2023 Feb;228(2):213.e1-213.e22. doi: 10.1016/j.ajog.2022.10.029. Epub 2022 Oct 29. (https://pubmed.ncbi.nlm.nih.gov/36414993)

Study Record Dates

These dates track the progress of study record and summary results submissions to ClinicalTrials.gov. Study records and reported results are reviewed by the National Library of Medicine (NLM) to make sure they meet specific quality control standards before being posted on the public website.

Study Registration Dates

First Submitted

2019-11-13

First Submitted that Met QC Criteria

2019-12-10

First Posted

2019-12-12

Study Record Updates

Last Update Submitted that Met QC Criteria

2024-07-01

Last Update Posted

2024-07-03

Last Verified

2024-07

More Information

Terms related to this study

Keywords Provided by Apple Inc.

Menstruation
Menstrual Cycle
Ovulation
Polycystic Ovary Syndrome
Infertility
Menopause
Reproduction
Reproductive Health

Additional Relevant MeSH Terms

Ovarian Cysts
Cysts
Neoplasms
Ovarian Diseases

Adnexal Diseases
Genital Diseases, Female
Female Urogenital Diseases
Female Urogenital Diseases and Pregnancy Complications
Urogenital Diseases
Genital Diseases
Gonadal Disorders
Endocrine System Diseases
Polycystic Ovary Syndrome
Infertility

Plan for Individual Participant Data (IPD)

Plan to Share Individual Participant Data (IPD)?

Undecided

Drug and device information, study documents, and helpful links

Studies a U.S. FDA-Regulated Drug Product

No

Studies a U.S. FDA-Regulated Device Product

No

P. EXHIBIT P: FTC REPORT

Exhibit: FTC (Report Number: 154835129)

Complaint against Apple Inc

From: Ashley Gjovik <ashleymgjovik@protonmail.com>

To opa@ftc.gov

Date: Friday, April 1st, 2022 at 11:39 PM

April 2nd, 2022

To Whom it May Concern,

This is a complaint against Apple Inc for unlawful data collection & invasion of employee privacy that spans years and multiple countries/continents, violating numerous laws and international agreements. While this complaint focuses on the rights of Apple's employees, the implications of Apple's violations for broader society should be self-evident.

I worked for Apple as a Senior Engineering Program Manager from February 2015 until my termination on September 9 2021, along with a Legal & Policy Internship working in Apple Products Legal in 2019. In August 2021, I expressed public concerns about Apple's overly restrictive/invasive employee polices, 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 (Gobbler/Glimmer) on employee's iPhones that automatically took photos/videos whenever it "thought it saw a face." I raised concerns about Apple's unlawfully invasive "Search and Privacy Policy" for employees, Apple's limitless access to employee's personal iCloud/Apple-server-based data, and Apple's culture of intimidation and secrecy (including a secret/private police force).

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

This 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, CERCLA, and OSHA statutes). 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. 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. Thus, I write to you today.

Please see attached legal memo for details.*

Thank you.

Respectfully,
-Ashley M. Gjovik

**Note: this complaint will also be submitted to the other government agencies, international bodies, and NGOs noted on page two.*

—
Ashley M. Gjøvik, J.D. Candidate, B.S., PMP
ashleygjovik.com | +1`415-964-6272

Sent with ProtonMail secure email.

2.46 MB 1 file attached

Gjovik v Apple - Privacy Complaint - Final.pdf 2.46 MB

Complaint has been submitted

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

To Ashley Gjovik<ashleymgjovik@protonmail.com>

Date Friday, December 30th, 2022 at 2:32 PMFriday, December 30th, 2022 at 2:32 PM

Your report has been submitted to the Federal Trade Commission.

Report Number: 154835129

Thank you for helping our work to protect consumers.

Learn about common scams and how to recover from them at ftc.gov/scams.
To file a report online, go to **ReportFraud.ftc.gov**.

FTC Next Steps

- We use reports to investigate and bring cases against fraud, scams, and bad business practices, but we can't resolve reports on behalf of individuals.
- We will share your report with our law enforcement partners.
- We use reports to spot trends, educate the public, and provide data about what is happening in your community. You can check out what is going on in your state or metro area by visiting **ftc.gov/exploredata**.

When we bring cases, we try to get money back for people. Check out **ftc.gov/refunds** to see recent FTC cases that resulted in refunds.

Additional Information

How to Avoid a Scam

Q. EXHIBIT Q: GERMANY & FRANCE

Complaints to German and French Privacy Authorities

BfDI Federal Commissioner for Data Protection and Freedom of Information

POSTAL ADDRESS The Federal Commissioner for Data Protection and Freedom of Information
PO box 1468, 53004 Bonn, Germany

STREET ADDRESS Graurheindorfer Straße 153, 53117 Bonn, Germany
PHONE +49 (0)228 997799-1117
E-MAIL Referat11@bfdi.bund.de
PERSON IN CHARGE Frau Wollnik
INTERNET www.bfdi.bund.de
DATE Bonn, 23.06.2022
FILE NUMBER 11-540 II#3693

Please always indicate the above file-number in all replies.

Ms
Ashley M. Gjovik

Only as e-mail:
ashleymgjovik@protonmail.com

SUBJECT **Your e-mail from 14. June 2022**

Dear Ms Gjovik,

Unfortunately, I have to inform you that we have handed over your submission to the responsible state data protection authority in Bavaria.

You can reach our colleagues as follows:

Bayerische Landesamt für Datneshcutzaufsicht

Promenade 18
91522 Ansbach

Telefon: 0981/180093-0

E-Mail: poststelle@lda.bayern.de

Homepage: https://www.lda.bayern.de

Best regards,
By order

Wollnik

54464/2022

DELIVERY ADDRESS Graurheindorfer Straße 153, 53117 Bonn, Germany
TRANSPORT CONNECTION Tram 61 and 65, Innenministerium
Bus 550 and SB60, Innenministerium

Re: Ihre Meldung vom 19.04.2022

From: Ashley Gjovik <ashleymgjovik@protonmail.com>

To poststelle@bfdi.bund.de<POSTSTELLE@bfdi.bund.de>

Date: Tuesday, June 14th, 2022 at 9:45 AM

Hello!

I wanted to check in on my question below.

I also want to let you know that a Germany journalist has been investigating this matter and found that these activities are occurring in Apple offices in Germany. The article should be published next week or the week after. I will share it when it is out. Is there a way for me to contact the investigator assigned to my case?

Thank you!
-Ashley

Hallo!

Ich wollte meine Frage unten überprüfen. Ich möchte Sie auch wissen lassen, dass ein deutscher Journalist diese Angelegenheit untersucht hat und festgestellt hat, dass diese Aktivitäten in Apple-Büros in Deutschland stattfinden. Der Artikel sollte nächste Woche oder die Woche danach veröffentlicht werden. Ich werde es teilen, wenn es draußen ist. Gibt es eine Möglichkeit für mich, den mit meinem Fall beauftragten Ermittler zu kontaktieren? Vielen

Dank! -Ashley

—
Ashley M. Gjøvik
Juris Doctor Candidate, International Law Scholar, B.S., PMP
ashleygjovik.com | +1 415-964-6272

"Never, ever be afraid to make some noise and get in good trouble, necessary trouble."
-U.S. Rep. John Lewis

Sent with Proton Mail secure email.

-------- Original Message --------
On Sunday, May 8th, 2022 at 8:51 PM, Ashley M. Gjøvik <ashleymgjovik@protonmail.com> wrote:

> Hello,
>
> Thank you very much. I would like to provide evidence for my charges, including: emails, documents, and photos.
>
> Is there a way for me to send these documents now? Or do I need to wait to hear from the investigator? Thank you!
>
> ---
>
> Google Translate / Google Übersetzer

> *Hallo! Vielen Dank. Ich möchte Beweise für meine Anklagen vorlegen, einschließlich: E-Mails, Dokumente und Fotos. Gibt es eine Möglichkeit für mich, diese Dokumente jetzt zu senden? Oder muss ich warten, um vom Ermittler zu hören? Vielen Dank!*

—
Ashley M. Gjøvik, J.D. Candidate, B.S., PMP
ashleygjovik.com | https://linktr.ee/ashleygjovik | +1 415-964-6272 (Signal)

Sent with ProtonMail secure email.

------- Original Message -------
On Tuesday, May 3rd, 2022 at 11:26 PM, POSTSTELLE@bfdi.bund.de POSTSTELLE@bfdi.bund.de wrote:

> Der Bundesbeauftragte für den Datenschutz
> und die Informationsfreiheit
> Az: 11-540/II#3693
>
> Sehr geehrte Frau Gjovik,
>
> zuständigkeitshalber haben wir Ihre Beschwerde an das Bayerische Landesamt für Datenschutzaufsicht weiter geleitet.
>
> Mit freundlichen Grüßen
> Im Auftrag
> Dustin Zeven
> **********
> Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
> Referat Z3
> Graurheindorfer Str. 153, 53117 Bonn
> Fon: (0228) 9977999316
> Fax: (0228) 99107799550
> E-Mail: referatz@bfdi.bund.de
> Internet: http://www.datenschutz.bund.de
> **********
> Datenschutzrechtliche Erklärung der BfDI für den E-Mail-Verkehr und die Erfüllung ihrer öffentlichen Aufgaben insgesamt (nachstehender Link führt auf den Internetauftritt der BfDI unter www.bfdi.bund.de)
>
> https://www.bfdi.bund.de/DE/Service/Datenschutzerklaerung/datenschutzerklaerung-node.html;jsessionid=43D7036B23C8e70B09F5B9B7804AFB99.2_cid329
>
> Kein Zugang für elektronisch signierte Dokumente
> **********
> Hinweis:
> Dies ist eine vertrauliche Nachricht und nur für den Adressaten bestimmt. Es ist nicht erlaubt, diese Nachricht zu kopieren oder Dritten zugänglich zu machen. Sollten Sie irrtümlich diese Nachricht erhalten haben, informieren Sie bitte sofort den Absender und vernichten diese E-Mail.

Case 3:23-cv-04597-EMC Document 30-1 Filed 03/13/26 Page 182 of 217
Case 3:23-cv-04597-EMC Document 27-6 Filed 05/20/2025 Page 100 of 414
(100 of 414), Page 100 of 414, Case: 25-2028, 05/20/2025, DktEntry: 27.6, Page 100 of 414

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Madame Ashley ASHLEYGJOVIK
1050 BENTON ST, 2310
95050 - SANTA CLARA, ETATS-UNIS

Lettre recommandée avec AR
N°AR : RW60 298 203 3 FR

Instruction du dossier :
Sophie GENVRESSE

Paris, le 09 JUIN 2022

N/Réf. : MLD/SGE/PZN/CLP221047
Saisine n°22006530
(à rappeler dans toute correspondance)

Madame,

Vous avez saisi la Commission nationale de l'informatique et des libertés (CNIL) d'une plainte à l'encontre de la société APPLE, concernant la collecte illicite de données personnelles et l'atteinte à la vie privée de ses salariés « *dans de nombreux pays* ».

En premier lieu, vous indiquez qu'APPLE impose l'installation et l'activation d'une application nommée « Gobbler » ou « Glimmer » sur le téléphone professionnel de ses salariés et collecte, par ce biais, des données "d'empreinte faciale" de chacun d'entre-eux, empreintes constituées à partir de photos et vidéos prises à leur insu. Ce traitement viserait à améliorer la fonctionnalité « Face ID ».

À cet égard, les éléments portés à notre connaissance ne nous permettent pas d'établir que le Règlement Général sur le Protection des Données (RGPD) trouverait à s'appliquer au traitement de données en cause.

En effet, je vous rappelle que l'article 3 du RGPD dispose que :

« 1. Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.

2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; où

b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif.
Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

Or, en l'espèce, le traitement semble être principalement effectué à Cupertino (Etats-Unis), au Canada ou en Israël. Il est par ailleurs mentionné dans la documentation interne d'Apple « *qu'aucune donnée de Glimmer ne doit être téléchargée en provenance de certaines régions* », plus précisément « *En France ni en Allemagne* » (Page 11 sur 54). D'après notre compréhension, dans l'hypothèse où l'application serait installée sur les appareils professionnels de salariés d'Apple en France (élément sur lequel nous ne disposons d'aucune information), les données collectées par l'application resteraient stockées localement, sur les téléphones professionnels des salariés.

En second lieu, vous nous indiquez qu'APPLE mettrait en œuvre un autre dispositif biométrique. Vous précisez en effet avoir reçu, depuis 2018, plusieurs emails d'APPLE vous invitant à participer à une étude dans laquelle des scans 3D haute résolution des oreilles des participants seraient réalisés. Aussi, vous précisez que le brevet " AirPods " de l'organisme décrit le dispositif comme un système permettant de capturer de nombreuses données de santé sur les utilisateurs, notamment le rythme cardiaque, le volume sanguin ou le rythme respiratoire des personnes concernées.

Concernant les données personnelles collectés dans le cadre du développement des « AirPods », votre réclamation se fonde uniquement sur le brevet déposé par Apple et plusieurs articles de presse en ligne, sans avancer d'autres preuves matérielles permettant d'attester que de tels traitements seraient mis en œuvre sur le territoire européen et/ou concernerait des personnes résidant dans l'Union Européenne.

Au regard de ce qui précède, les traitements de données à caractère personnel objets de votre saisine n'apparaissent donc pas relever du champ d'application territorial du RGPD.

Au demeurant, j'attire votre attention sur le fait que, pour les traitements qui relèvent du RGPD, l'autorité compétente pour en connaître est l'autorité de contrôle cheffe de file, c'est-à-dire l'autorité où se situe l'établissement principal du responsable de traitement. En l'occurrence, s'agissant d'Apple, il s'agirait de l'autorité irlandaise. Ainsi, et sauf à ce que le traitement de données à caractère personnel en cause ne soit pas transfrontalier et soumis au mécanisme de coopération prévu par le RGPD, la CNIL n'a en principe pas compétence pour contrôler les traitements mis en œuvre par APPLE.

Nous prenons néanmoins bonne note des éléments communiqués et resterons attentifs à d'éventuels compléments ou évolution conduisant à considérer que de tels traitements constituent une violation de la réglementation française ou européenne en matière de protection des données.

Je vous prie d'agréer, Madame, l'expression de mes salutations distinguées.

Marie-Laure DENIS
Présidente

Sous réserve de l'intérêt pour agir des requérants, les décisions de la CNIL sont susceptibles de faire l'objet d'un recours devant le Conseil d'Etat dans un délai de deux mois à compter de leur notification.

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS
3 Place de Fontenoy
TSA 80715
75334 PARIS
CEDEX 07

PRIORITAIRE
PRIORITY
Document

PARIS
75
10 06 2
883 I1 0M 064
FFF3 752330

€ R.F.
008,20
LA POSTE
CP 651372

RW 60 298 203 3 FR
FRANCE
RW 60 298 203 3 FR
PRIO
RECOMMANDÉ / REGISTERED

LA POSTE
FRANCE

Destinataire de l'envoi (nom, prénom, adresse) :
Ashley GSOVIK
1050 BENTON ST., 2310
95050 - SANTA CLARA
ETATS-UNIS

A remplir par l'expéditeur

courrier | colissimo | livre | sac M | montant Valeur déclarée :

mandat n° : | montant :

A remplir par le bureau de dépôt

À compléter à destination / To be completed at destination :

L'(envoi) mentionné ci-dessus a été dûment :
This item has been duly :

Remis / Delivered | Payé / Paid

Date et signature / Day of delivery and signature *

* Cet avis pourra être signé par le destinataire ou, si les règlements du pays de destination le prévoient, par une autre personne autorisée ou par l'agent du bureau de destination.
This item has to be signed by the addressee, (if it's authorized by the regulation of country of destination) by someone else authorized, or by the postal worker at destination.

Service des Postes
AVIS DE RÉCEPTION

PRIORITAIRE / PAR AVION
AVIS DE PAIEMENT

N° de l'envoi : RW 60 298 203 3 FR

Timbre du bureau renvoyant l'avis
Stamp of the Post Office returning the advice

MLD/SGE/PZN/CLP EE1047

CNIL - Commission Nationale de l'Informatique et des Libertés
3 Place de Fontenoy
TSA 80715
75 334 PARIS CEDEX 07

FRANCE

Zone réservée au traitement Poste

(92 of 414), Page 92 of 414 Case: 25-2028, 05/20/2025, DktEntry: 27.6, Page 92 of 414

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Ms Ashley ASHLEY GJOVIK
1050 BENTON ST, 2310
95050 - SANTA CLARA, UNITED STATES

Registered letter with acknowledgement of receipt
N°AR :RW60298 203 3 FR

lnstniction du dossier :
Sophie GENVRESSE

Paris, le 09 June 2022

Ref. number: MLD/SGE/PZN/CLP221047
Referral n°22006530
(to be included in all correspondence)

Madam,

You have lodged a complaint with the French Data Protection Authority (Commission nationale de l'informatique et des libertés - CNIL) against APPLE, concerning the illicit collection of personal data and the invasion of the privacy *of* its employees « in many countries ».

Firstly, you state that APPLE requires its employees to install and activate an application called "Gobbler" or "Glimmer" on their work phones, thereby collecting "facial imprint" data from photos and videos taken without their knowledge. The aim is to improve Face ID functionality.

In this respect, the elements brought to our attention do not allow us to establish that the General Regulation *on* Data Protection (RGPD) would find application to the data processing in question.

Indeed, I remind you that Article 3 of the RGPD states that.

" 1. This Regulation shall apply to the processing of personal data carried out in the course of the activities of a controller or of a service provider within the territory of the Union, whether or not the processing takes place within the Union.

2. The present regulation applies to the processing of personal data relating to the persons concerned who are on the territory of the Union by a processing re.open.battle or soas-truitunt which is not established in the Union, where the processing activities are linked to - the processing of personal data relating to the persons concerned who are on the territory of the Union by a processing re.open.battle or soas-truitunt which is not established in the Union, where the processing activities are linked to - the processing of personal data relating to the persons concerned who are on the territory of the Union.

a) the offering of goods or services to such data subjects in the Union, whether or not a payment is required from them; or
b) the monitoring of their behavior, insofar as such behavior takes place within the Union.

The personal data required to carry out CNIL's missions are treated as data for its exclusive use.
co-accredited persons may assert their tri/ormotor and legal rights by contacting the CNIt's data protection delegate iOPOJ.
-'- --f-< ulaire en 1+que ou par courrier posiol. Potir et savoir glus , 'wow.cnitfr/doniiees-oersontie1les.

However, in this case, processing appears to be carried out mainly in Cupertino (United States), Canada, or Israel. Apple's internal documentation also states that "*no Glimmer data should be downloaded in certain regions.*" More specifically, "*In France or Germany*" (page 11 of 54). According to our understanding, in the event that the application were to be installed on the professional devices of Apple employees in France (about which we have no information), the data collected by the application would remain stored locally on the employees' professional phones.

Secondly, you indicate that APPLE is implementing another biometric device. You specify that, since 2018, you have received several emails from APPLE inviting you to participate in a study in which high-resolution 3D scans of participants' ears would be taken. You also specify that the "AirPods" patent describes the device as a system capable of capturing a wide range of health data on users, including heart rate, blood volume and breathing rate.

Regarding the personal data collected in connection with the development of "AirPods," your complaint is based solely on the patent filed by Apple and several online press articles, without providing any other material evidence to support the claim that such tracking is being carried out in the European Union and/or affects individuals residing in the European Union.

In light of the above, the processing of personal data that is the subject of your referral does not appear to fall within the territorial scope of the GDPR.

Furthermore, I would like to draw your attention to the fact that, for processing operations falling within the scope of the GDPR, the competent authority is the lead supervisory authority, i.e. the authority where the data controller has its main establishment. In this case, as it concerns Apple, would be the Irish authority. Therefore, unless the processing of personal data in question is cross-border and subject to the cooperation mechanism provided for by the GDPR, the CNIL does not, in principle, have jurisdiction to supervise the processing carried out by APPLE.

We nevertheless take note of the information provided and will remain attentive to any additional information or developments that could lead us to consider that such processing constitutes a violation of French or European data protection regulations.

Yours sincerely



Marie-Laure DENIS President

Subject to appeal by the applicants, the decisions of the CNIL may be appealed to the Council of State within two months of their notification.The decisions of the CNIL may be appealed to the Council of State within two months of their notification.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Madame Ashley ASHLEYGJOVIK
1050 BENTON ST, 2310
95050 SANTA CLARA

Paris, le 5 avril 2022

Accusé de réception de votre courrier

Votre numéro de dossier : 22006530
(à rappeler lors de tout contact avec la CNIL)

Nous avons bien reçu votre demande le 02 avril 2022.

Après analyse de sa recevabilité, elle a été transmise pour instruction au service des plaintes de la CNIL qui vous informera de l'état d'avancement de votre dossier.
A cette occasion, des éléments complémentaires pourront vous être demandés.

Lorsque 3 mois se seront écoulés, pour savoir où en est votre dossier, vous pourrez nous contacter en précisant le numéro figurant sur le présent accusé de réception, sur le site de la CNIL depuis le formulaire de la rubrique Besoin d'aide « Comment savoir où en est ma réclamation? ».

Si dans le délai de 3 mois vous avez d'éventuels compléments à apporter, vous pouvez également utiliser ce même formulaire en ligne.

Nous appelons votre attention sur le fait que les délais de traitement peuvent être importants en raison du grand nombre de saisines que nous recevons.

Au terme de l'instruction, vous serez informé de l'issue de votre dossier.

Le Service des Relations avec les Publics

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont conservées et traitées dans des fichiers destinés à son usage exclusif.
Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

CNIL.
CODE I¥SION NATIONALE IN
FORMATIQTJE & LIBERTÉS

Mrs Ashley ASHLEYGJOVIK 1050
BENTON ST, 2310
95050 SANTA CLARA

Paris, April 5, 2022

Your file number: 22006530
*(to be remembered when contacting **the CNIL**)*

We received your request on April 02, 2022.

After analysis of its admissibility, it was forwarded to the complaints department for processing. of the CNIL, which will keep you **informed** of the progress **of your case.**
You may be asked to provide additional information.

When 3 months have elapsed, to find out the status of your claim, you can contact us by specifying the number shown on this acknowledgement of receipt, on the CNIL website from the form in the Need help section "How to find out the status of my claim†".

If you need to make any additions within 3 months, you can also use the same online form.

We would like to draw your attention to the fact that processing times can be long due to the large number of referrals we receive.

At the end of the instruction, you will be informed of Pissne dewtre dmsier.

Public Relations Department

The Wayback Machine - https://web.archive.org/web/20230105104914/https://www.cnil.fr/en/advertising-id-apple-dist…

Advertising ID: APPLE DISTRIBUTION INTERNATIONAL fined 8 million euros

04 January 2023

On 29 December 2022, the CNIL's restricted committee imposed an administrative fine of 8 million euros on the company APPLE DISTRIBUTION INTERNATIONAL because it did not collect the consent of iPhone's French users (iOS 14.6 version) before depositing and/or writing identifiers used for advertising purposes on their terminals.

Background information

Following a complaint concerning the ad personalization in the App Store, the CNIL carried out several investigations in 2021 and 2022 in order to verify compliance with the applicable regulations.

The CNIL services found that under the old version 14.6 of the operating system of the iPhone, when a user visited the App Store, identifiers used for several purposes, including personalization of ads on the App Store, were by default automatically read on the terminal without obtaining consent.

The breach of the French Data Protection Act

Due to their advertising purpose, these identifiers are not strictly necessary for the provision of the service (the App Store). Therefore, they must not be read and/or deposited without the user's prior consent. However, in practice, the advertising targeting settings available from the "Settings" icon of the iPhone were pre-checked by default.

Moreover, the user had to perform a large number of actions in order to deactivate this setting, since this option was not included in the initialization process of the phone. Therefore, the user had to click on the "Settings" icon of the iPhone, then go to the "Privacy" menu and finally to the section entitled "Apple advertising". These elements did not allow to collect the prior consent of users.

Consequently, the restricted committee, the CNIL's body responsible for issuing sanctions, found a breach of Article 82 of the French Data Protection Act and imposed a fine of 8 million euros on APPLE DISTRIBUTION INTERNATIONAL, which was made public.

It explained this amount by the scope of the processing limited to the Apple Store, the number of people concerned in France, the profits the company made from advertising revenues indirectly generated from data collected by these identifiers and the fact that since then, the company has reached compliance.

Jurisdiction of the CNIL

The CNIL is **materially competent** to verify and sanction operations related to identifiers deposited and/or read by the company on the terminals of Internet users located in France. The cooperation mechanism provided for by the GDPR (the “one-stop shop” mechanism) is not intended to apply in these procedures insofar as the operations linked to the use of the identifiers fall within the scope of the " ePrivacy " directive, transposed in Article 82 of the French Data Protection Act.

The restricted committee considered that the CNIL is also **territorially competent** because the use of identifiers is carried out within the "framework of the activities" of the companies APPLE RETAIL FRANCE and APPLE FRANCE, which constitute the "establishments" on French territory of the APPLE group.

Note: APPLE DISTRIBUTION INTERNATIONAL*, whose head office is in Ireland, presents itself as the controller of the processing regarding the ad personalization on the App Store, in the European region. The companies APPLE RETAIL FRANCE and APPLE FRANCE are the establishments in France of the Apple group.*

Texte reference

The decision (in French)

> Délibération de la formation restreinte n°SAN-2022-025 du 29 décembre 2022 concernant la société APPLE DISTRIBUTION INTERNATIONAL - Légifrance
Texte reference

Pour approfondir

> The sanctions procedure
> [FR] Identifiant publicitaire : sanction de 8 millions d’euros à l’encontre de APPLE DISTRIBUTION INTERNATIONAL
Haut de page

R. EXHIBIT R: FEB. 4 2026 EMAIL

See also, Ex. from Declaration in Support of Plaintiff's Motion for Sanctions at Dkt. 302-1 (03/06/26) pp. 9-28, incorporated here.

Re: (Ashley Gjovik v. Apple, Inc.)(126432) – Deposition Transcript Designations

From Ashley M. Gjovik (Legal Matters) <legal@ashleygjovik.com>

To Ashley Gjovik<ashleymgjovik@protonmail.com>

CC Mantoan, Kathryn G.<kmantoan@orrick.com>, Riechert, Melinda<mriechert@orrick.com>, Perry, Jessica R.<jperry@orrick.com>, Horton, Nicholas J.<nhorton@orrick.com>, Booms, Ryan<rbooms@orrick.com>

Date Wednesday, February 4th, 2026 at 6:15 PM

Attn: new NLRB charge

Hello,

I'm removing Talty from this thread and I'm going to ask you one more time to meet/confer with me on this, because you have refused to meet/confer on this, you waited well past the 30-day deadline for substantiating your claims, and the document you sent tonight contains content that violates state and federal law -- including at least labor, whistleblower, consumer, privacy, medical, and professional ethics laws.

Certainly you had to expect that I would complain about Apple claiming my own menstruation, cervical mucus, and sexual activity are "Apple Confidential."

You also must have known that I would be further disgusted to see Apple claim that my complaints about Apple invading my, and my coworkers, privacy rights regarding menstruation, cervical mucus, and the people we choose to have sexual intercourse with in our own homes is also "Apple Confidential" so our complaints about privacy violations by Apple, and Apple's underlying conduct, are somehow secret.

You also know that in my lawsuit and some of the administrative proceedings, I cite these exact topics as protected disclosures, concrete harms/injuries, unfair business practices, and/or work conditions -- and I allege Apple's own conduct is unlawful, harmful, and requiring enforcement action including injunctive relief.

You have refused to even attempt to justify these confidentiality claims, disregarded and refused to comply with the exact process you insisted be put in place and where you had promised confidentiality disputes would be addressed, and instead you have now taken action to formalize and permanently record your client's illegal assertions.

Further, this deposition is about my employment at Apple, my concerns about work conditions and the rights of Apple employees generally, and its partially in response to my claims of unlawful labor practices -- which means that Apple's about to get a new NLRB charge filed against it, arising from your document today.

While NLRB has resisted taking action that could interfere with standard court procedures in this case, here Apple has chosen to refuse to engage with standard court procedures, cut off my access to standard procedures, and is literally claiming in an official legal document that Apple thinks it has some sort of vested business interest and secrecy claim to its employees... genital secretions.

So even an NLRB run by Apple's own lawyer will have a hard time dismissing this one -- unless, maybe if you come to the table and actually participate in this process in good faith.

I stress again, you're not even attempting to offer some nonsense, vague justification for these claims -- you're just refusing to engage in the process completely while concurrently threatening to take unjustified actions to further invade my privacy, interfere with my exercise of my privacy rights and right to bodily autonomy, and to implicitly threaten other employees to not engage in the same protected activity that I did including reporting retaliation and harassment by Apple. That sounds illegal!

So let me know if we do a video call or phone call or something where we can actually at least pretend to meet/confer about this -- or if you're just going sticking to your current path of claiming that Apple has intellectual property rights over their worker's vaginas -- because that's where we're at tonight and its extremely disturbing.

—

Ashley M. Gjøvik

BS, JD, PMP

Sent with Proton Mail secure email.

On Wednesday, February 4th, 2026 at 4:39 PM, Ashley M. Gjøvik <ashleymgjovik@protonmail.com> wrote:

> Apple counsel,
>
> I sent you an email about this a few moments ago (re-adding below) and instead of replying to me, you sent your own email not addressed to me, ccing me as an observer, and you are asserting a process that does not comply with the Protective Order we signed for Discovery. That means you are in violation of that Order and refusing to comply with the process you insisted on for this case.
>
> You need to send **me** your claims and then we are to meet/confer about those claims.
>
> Talty Ho is not the Magistrate Judge in our case and will not be deciding the validity of claims.
>
> Once we agree to the claims, then they should be reflected in the transcript -- and you were supposed to do this with me over a month ago.
>
> I ask that you send me your claims to discuss -- as of now you have expressly excluded me from your claims and are attempting to formalize your claims without my input, despite my direct request to you to meet/confer about exactly this.
>
> —
> **Ashley M. Gjøvik**
> **BS, JD, PMP**
>
> Sent with Proton Mail secure email.
>
> On Wednesday, February 4th, 2026 at 4:32 PM, Mantoan, Kathryn G. <kmantoan@orrick.com> wrote:

Talty CR Production Team:

I write regarding the deposition transcript we received on 1/7/2026 in this matter.

Pursuant to the operative Protective Order, we have reviewed the transcript and are finalizing our confidentiality designations. Attached is a chart identifying the specific portions (with citations and text) for which confidentiality is being asserted.

Plaintiff is copied on this email for notice purposes.

Thank you,

Katie

Kathryn G. Mantoan

Attorney

Pronouns: she / her / hers

Orrick

San Francisco | Portland

T +1-415-773-5887
M +1-415-218-4865
T +1-503-943-4870
kmantoan@orrick.com

NOTICE TO RECIPIENT | This e-mail is meant for only the intended recipient of the transmission, and may be a communication privileged by law. If you received this e-mail in error, any review, use, dissemination, distribution, or copying of this e-mail is strictly prohibited. Please notify us immediately of the error by return e-mail and please delete this message from your system. Thank you in advance for your cooperation.

In the course of our business relationship, we may collect, store and transfer information about you. Please see our privacy policy at https://www.orrick.com/Privacy-Policy to learn about how we use this information.

On Wednesday, February 4th, 2026 at 4:22 PM, Ashley M. Gjøvik <ashleymgjovik@protonmail.com> wrote:

> Hello,
>
> I'm adding Apple to this thread.
>
> Apple's counsel,
>
> We need to complete our review of the transcript, submit any corrections, and ensure that we don't then need more corrections based on the other party's corrections.
>
> We also need to finalize the Confidentiality claims and ensure the record accurately represents those claims including for any exhibits. I asked you for updates on your Confidentiality claims and you said you were working on it but I have yet to see any updates from you -- and nothing to actually narrow, define, and substantiate any of your Confidentiality claims.
>
> The deposition was nearly two months ago and during the deposition I told you to substantiate any Confidentiality claims and that I was not agreeing to any blanket Confidentiality claims.
>
> Under the Protective Order you have a limited amount of time to substantiate your claims and if you do not, they are waived. Under that order, for this deposition, all of your Confidentiality claims would be waived by now.
>
> However, there's probably at least a few statements/terms that are plausibly Confidential, I am still bound by the lawful/legitimate terms within the NDAs I consented to and signed, and I feel it would be proper to allow Apple to still substantiate the things that may actually be Confidential.
>
> That said, you're already overdue and I need a timeline from you as to when you will be done and to ensure it can still be reflected in this deposition transcript.
>
> I also ask if you're submitting any requests for corrections to this records, and if so, to please share with me what you ask for.
>
> I also need to submit my request for corrections so please let me know if you'd like any process for that other then being cc'd or receiving a copy of what I submit to the Talty team.
>
> -Ashley

—
Ashley M. Gjøvik
BS, JD, PMP

Sent with Proton Mail secure email.

3.90 KB 2 embedded images

S. EXHIBIT S: BLOG POST

Exhibit: ***"Apple Claims It Owns Its Employees' Cervical Mucus: A New NLRB Charge Reveals the Logical Endpoint of Corporate Confidentiality Abuse"***

See Ex. B from Plaintiff's Objections at Dkt. 284 (2/20/26) pp. 70-84, incorporated here.

T. EXHIBIT T: SOCIAL MEDIA POST

Exhibit: Social Media Posts
See Ex. C from Plaintiff's Objections at Dkt. 284 (2/20/26) pp. 85-95, incorporated here.

EXHIBIT:
DECLARATION OF THOMAS LE BONNIEC

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

ASHLEY GJOVIK,
an individual,
Plaintiff/Appellant,
v.

APPLE INC,
a corporation,
Defendant/Appellee.

Case No. 25-2028

Declaration of Thomas le Bonniec

DECLARATION OF THOMAS LE BONNIEC IN SUPPORT OF ASHLEY GJOVIK'S REQUEST FOR APPEAL AND MOTION FOR INJUNCTIVE RELIEF

Pursuant to 28 U.S. Code § 1746, I, Thomas Le Bonniec, declare as follows:

1. My name is Thomas Le Bonniec. I make this declaration of my own personal knowledge, and if called to testify in Court on these matters, I could do so competently under oath to such facts. I make this declaration in support of Plaintiff's Opposition to Apple's Motion to Dismiss her Third Amended Complaint.

2. I contacted Plaintiff, Ashley Gjovik, in November of 2022. I wanted to speak with her about [stuff]. Plaintiff responded in November 2022, and since then, she and I have emailed and also met several times for video conversations. We often discuss our concerns about consumer privacy. I shared with Plaintiff what I saw working at an Apple subcontractor, and Plaintiff shared with me her experience with Apple's "Gobbler" application and other data collection practices performed Apple that bothered her. We have often spoke about how important the right to privacy is to us, and complained about statements made by Apple about privacy which we felt were deceptive based on our own firsthand experiences with the company. Plaintiff and I have also discussed how fearful we both were and are to speak out against Apple.

3. During my conversations with Plaintiff, she shared with me some of the negative experiences that have occurred to her after she reported Apple to the US and California governments. The statements Plaintiff made to me contained specific allegations and were consistent with her statements under her RICO Act, Bane Act, Ralph Act, and IIED claims in her Third Amended Complaint. Plaintiff has also expressed to me her fear and reluctance to continue to act as a witness against Apple due to the negative events she has experienced.

4. Plaintiff's Third Amended Complaint alleged that, in violation of the U.S. RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT, that Apple was

intentionally creating a "*knowingly false reputation of strong regulatory compliance*" and is engaging on "*intimidation*" of potential "*witnesses*." [docket #47]

5. Apple disputes this point in its Motion to Dismiss [docket #48, page 14, lines 5-8] Apple wrote that Plaintiff's Third Amended Complaint did adequately state "*what role Apple or any other entity played in concocting the alleged scheme or ensuring its and success*." docket #48, page 18, lines 1-9]. Apple also argued that Plaintiff "*does not identify any other 'witness'*." [docket #48, page 19, lines 3-9].

6. I offer this declaration in support of Plaintiff's claims. I was a witness to, what I feel was, violations of multiple laws by Apple – and also a witness to, what I feel, was a scheme by Apple to conceal the acts and intimidate witnesses from reporting Apple's activities. What I witnessed occurred in Cork, Ireland during 2019 while I worked for Global Technical Services Ltd. ("GlobeTech"), a subcontractor of Defendant Apple Inc.

7. On May 8th, 2019, I signed a Non-Disclosure Agreement and an employment agreement with GlobeTech. [Exhibit A]. I worked in the position of "Data Analyst" at Globetech. My job consisted of listening to audio files recorded by Apple's products and to verify and correct the written transcription from "Siri," Apple's vocal assistant.

8. I witnessed thousands of audio recordings of the public, captured by Apple's devices all over the world, and stored on service where we could listen to the actual audio recordings. I witnessed recordings in situations like a person talking about their political opinion, kids talking to their iPad, and others dictating private messages about their health state. I also heard a man playing out loud his sexual fantasies with young children.

9. The employee guidelines provided to me by GlobeTech stated: "*Be aware that this project will involve private and personal user data. Vulgar language, violent themes, pornographic or criminal subjects may show up. If this is too disturbing, please speak to your manager*." [attached as Exhibit C is a true and correct image of the message noted which I captured myself while still employed at GlobeTech]

10. This activity was conducted on Apple's hardware (MacBooks), through Apple's Virtual Private Network, and on Apple's platform ("CrowdCollect"). [attached as Exhibits D and E are true and correct images of the "CrowdCollect" tool, which I captured myself while still employed at GlobeTech]. I was also provided a @apple.com Apple corporate email address.

11. While I worked at GlobeTech analyzing the recordings, in addition to the NDA I signed, I also witnessed managers telling me and other workers that GlobeTech expected us to remain silent and not speak with each other during our

shift. I also witnessed a manager telling me and others to not tell anyone about our work, even our family or friends, and they said, especially journalists. I desperately wanted to talk to my coworkers about the ethics of what we were doing, but due to these rules, I felt it was very difficult to do so.

12. I felt that that Apple's recordings of these private conversations was unethical, so I left GlobeTech without prior notice. I did not want to participate in what I felt could be unlawful activity. I received after a few days a notice of termination of employment due to my absence.

13. In 2019, I engaged with European media outlets to share my experience. In 2020, after resigning, I filed several complaints with the European Data Protection Authorities and with the U.S. Securities and Exchange Commission attesting to what I saw and experienced in my position at GlobeTech.

14. One specific issue I raised to the US SEC was how Apple and GlobeTech asked GlobeTech workers to sign non-disclosure agreements which I felt were intimidating and too restrictive. I felt that the wording of the NDA implied I could not communicate with law enforcement agencies about what I witnessed related to Apple's audio recordings without a risk of retaliation, including being sued by Apple. [See Exhibit A, page 4, section "5.6 Remedies"].

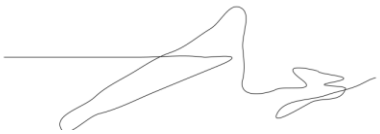
15. I have publicly stated that these NDAs have a chilling effect and I believe they are intended to intimidate workers who are witnesses of potentially

unlawful conduct by Apple, and which is facilitated by Apple's external business partners, like GlobeTech. [attached as Exhibit B is a true and correct copy of a Bloomberg article I was interviewed for and quoted it]

16. Despite my fear of retaliation for reporting what I saw, which I did and do have, I felt compelled to report, as I felt it was an ethical obligation, despite the EU authorities' absence of reaction. I was also motivated to speak out after reading about other Apple whistleblowers who also came forward to speak about these Siri recordings a few days before I did. I read about these whistleblowers in articles including in The Guardian on July 26th, 2019 [attached as Exhibit F is a true and correct image of the article noted] and El Pais on July 26th, 2019 [attached as Exhibit G is a true and correct image of the article noted]. I was and am concerned that I witnessed Apple's audio recording practices still occurring in 2019-2020, even after those other whistleblowers came forward in 2019 before me.

17. On February 14th , 2025 on the basis of my testimony and the evidence I provided, a complaint was filed by the Human Rights League in France for these privacy violations (exhibit H).

18. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.



Executed this 12TH day of May 2025

in Paris, France.

_____

Thomas LE BONNIEC

EXHIBIT A: GLOBETECH NDA

CONFIDENTIALITY AGREEMENT

BETWEEN:

GLOBE TECHNICAL SERVICES LIMITED, a company registered under the laws of Ireland with company no. 277495 and its registered office at Building 6900, Cork Airport Business Park, Cork, Ireland.

and

Thomas Le Bonniec

SUMMARY OF CONFIDENTIALITY OBLIGATIONS

A. You must keep all Confidential Information you receive while working with us strictly confidential.
B. You may only discuss or share Confidential Information with those individuals who are authorized to work on the project that the Confidential Information relates to or your manager. You should seek permission from your manager before discussing or sharing Confidential Information with anyone else.
C. Confidential Information should not be discussed in open plan areas, coffee areas, corridors or public places or where there is a possibility of being overheard.
D. You should never discuss Confidential Information outside of work.
E. If you have any doubts about your obligations ask your manager.
F. Failure to comply with the provisions of this Agreement may result in personal liability.

This confidentiality agreement (the "**Agreement**") will apply in addition to any terms and conditions agreed between the parties provided that this Agreement shall take precedence in all circumstances in the event of any conflict.

In consideration and as a condition of my continued relationship, whether as an officer, director, employee or consultant with Globe Technical Services Limited and any of its related companies (the "**Company**") I agree as follows:

1. WHAT IS CONFIDENTIAL INFORMATION?

1.1. Confidential Information means information:
1.1.1. in whatever form (including, without limitation, in spoken, written, visual or electronic form or on any magnetic or optical disk or memory and wherever located); and
1.1.2. relating to the business, products, affairs and finances of the Company or any of its customers or suppliers and trade secrets including, without limitation, technical data and know-how relating to the business of the Company; and

1.1.3. relating to any of the Company's suppliers, clients, customers, agents, distributors, shareholders or management whether or not such information is marked or designated as confidential; and

1.1.4. that is marked or otherwise identified as confidential or proprietary, or that would otherwise appear to a reasonable person to be (reasonably) confidential or proprietary in the context and circumstances in which the information is known or used.

1.2. Confidential Information does not include information that is:

1.2.1. available to the public generally; or

1.2.2. required to be provided in response to a valid order by a court or other governmental body or otherwise required by law.

2. WHAT ARE MY CONFIDENTIALITY OBLIGATIONS?

I will handle Confidential Information in a confidential manner at all times and commit to the following obligations:

2.1. ***General Confidentiality Obligations***

2.1.1. to treat all Confidential Information as strictly confidential;

2.1.2. to use and disclose Confidential Information only in connection with and for the purpose of performing my assigned duties;

2.1.3. not to take pictures or videos or use recording devices while on site with a customer of the Company;

2.1.4. to ensure that Confidential Information is not discussed in open plan areas, coffee areas, corridors or public places or where there is a possibility of being overheard. A reasonably sound proofed room should be used when discussing Confidential Information and all windows and doors should be closed;

2.1.5. to only make such hard or electronic copies of any Confidential Information as are absolutely necessary for performing my assigned duties. If any hard copies are made of Confidential Information these should be clearly labelled as such and treated accordingly;

2.1.6. to only discuss Confidential Information with those that I have been informed are authorized to receive it;

2.1.7. to request, obtain or communicate Confidential Information only as necessary to perform my assigned duties and refrain from requesting, obtaining or communicating more Confidential Information than is necessary to accomplish my assigned duties;

2.1.8. in any event, not to speak of, discuss or communicate Confidential Information outside of the work environment, including, to family members and friends; and

2.1.9. not to access or use any Confidential Information, and not to copy any documents, records, files, media or other resources containing any Confidential Information, or remove any such documents, records, files, media or other resources from the premises or control of the Company, except with the prior consent of an authorized officer acting on behalf of the Company in each

instance (and then, such disclosure shall be made only within the limits and to the extent of such duties or consent).

2.2. ***Security & Access Confidentiality Obligations***

2.2.1. to take utmost care to properly secure Confidential Information on my computer and to take steps to ensure that others cannot view or access such Confidential Information. When I am away from my workstation or when my tasks are completed**,** I will log off my computer or use a password-protected screensaver in order to prevent access by unauthorized users;

2.2.2. not to disclose my personal password(s) to anyone without the express written permission of my department head or record or post it in an accessible location and refrain from performing any tasks using another person's password;

2.2.3. to comply with all Company security policies and procedures as in force from time to time relating to the use of Company equipment, software, data (including Confidential Information) and systems ("**Company Technology Resources**");

2.2.4. not to access or use any Company Technology Resources except as authorized by Company; and

2.2.5. not to access or use any Company Technology Resources in any manner after the termination of my role, whether termination is voluntary or involuntary. I agree to notify Company promptly in the event I learn of any violation of the foregoing by others, or of any other misappropriation or unauthorized access, use, reproduction or reverse engineering of, or tampering with any Company Technology Resources or other Company property or materials by others.

2.3. ***Exit Confidential Obligations***

2.3.1. Upon voluntary or involuntary termination of my role or the Company's request at any time, I shall provide or return to the Company any and all Company property, including keys, key cards, access cards, identification cards, security devices, Company credit cards, network access devices, computers, cell phones, smartphones, PDAs, equipment, manuals, reports, files, books, compilations, work product, e-mail messages, recordings, tapes, disks, thumb drives or other removable information storage devices, hard drives, and data and all Company documents and materials belonging to the Company and stored in any fashion, including but not limited to those that constitute or contain any Confidential Information or work product, that are in my possession or control, whether they were provided to me by the Company or any of its business associates or created by me.

3. WHO OWNS CONFIDENTIAL INFORMATION AND OTHER MATERIALS?

3.1. You may in the course of working with the Company, conceive, develop or contribute to material or information related to your assigned role or the business of the Company, including, without limitation, software, technical documentation, ideas, inventions (whether or not patentable), hardware, know-how, marketing plans, designs,

Exhibit A

techniques, documentation and records, regardless of the form or media, if any, on which such is stored (referred to in this Agreement as "**Proprietary Information**"). The Company shall exclusively own all Proprietary Information which you conceive, develop or contribute to in the course of working with the Company and all intellectual and industrial property and other rights of any kind in or relating to the Proprietary Information, including but not limited to all copyright, patent, trade secret and trade-mark rights in or relating to the Proprietary Information. You agree to assign to the Company any and all rights that you may have or obtain in or to the Proprietary Information. If you conceive, develop or contribute to material or information outside work hours on the Company's premises or through the use of the Company's property and/or assets shall also be Proprietary Information and be governed by this Agreement if such material or information relates to the business of the Company. You shall keep full and accurate records accessible at all times to the Company relating to all Proprietary Information and shall promptly disclose and deliver to the Company all Proprietary Information.

4. HOW LONG DO THESE OBLIGATIONS LAST?

The obligations under this Agreement with regard to any particular Confidential Information shall commence immediately when you first have access to such Confidential Information and shall continue during and after termination or your role until such time as such Confidential Information has become public knowledge other than as a result of your breach of this Agreement or breach by those acting in concert with you or on your behalf.

5. GENERAL PROVISIONS

5.1. **No Assignment**. You shall not assign or transfer any rights or obligations under this Agreement without the prior written consent of Company.

5.2. **Notices**. Any notice required or permitted by this Agreement shall be in writing to the addresses set forth above or such other address as either party may specify in writing.

5.3. **Governing Law**. This Agreement shall be governed in all respects by the laws of the Republic of Ireland and the courts in the Republic of Ireland shall have exclusive jurisdiction.

5.4. **Severability**. Should any provisions of this Agreement be held by a court of law to be illegal, invalid or unenforceable, the legality, validity and enforceability of the remaining provisions of this Agreement shall not be affected or impaired thereby.

5.5. **Waiver**. The waiver by Company of a breach of any provision of this Agreement shall not operate or be construed as a waiver of any other or subsequent breach.

5.6. **Remedies**. You acknowledge that the Confidential Information and the Company's ability to reserve it for the exclusive knowledge and use of the Company is of great competitive importance and commercial value to the Company, and that improper use or disclosure of the Confidential Information will cause irreparable harm to the Company for which remedies at law will not be adequate.

5.7. In the event of a breach or threatened breach by you of any of the provisions of this Agreement, you hereby consent and agree that the Company shall be entitled to, in

Exhibit A

addition to other available remedies, a temporary or permanent injunction or other equitable relief against such breach or threatened breach from any court of competent jurisdiction, without the necessity of showing any actual damages or that monetary damages would not afford an adequate remedy, and without the necessity of posting any bond or other security. Any equitable relief granted shall be in addition to, not in lieu of, legal remedies, monetary damages or other available forms of relief. You agree that each customer of Company is an intended third-party beneficiary of this Agreement so that customers of Company may enforce the provisions of this Agreement against you.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date last written below:

Globe Technical Service Limited

Emma Flynn

By: HR Representative

Title: HR Administrator

Dated: 08/05/2019

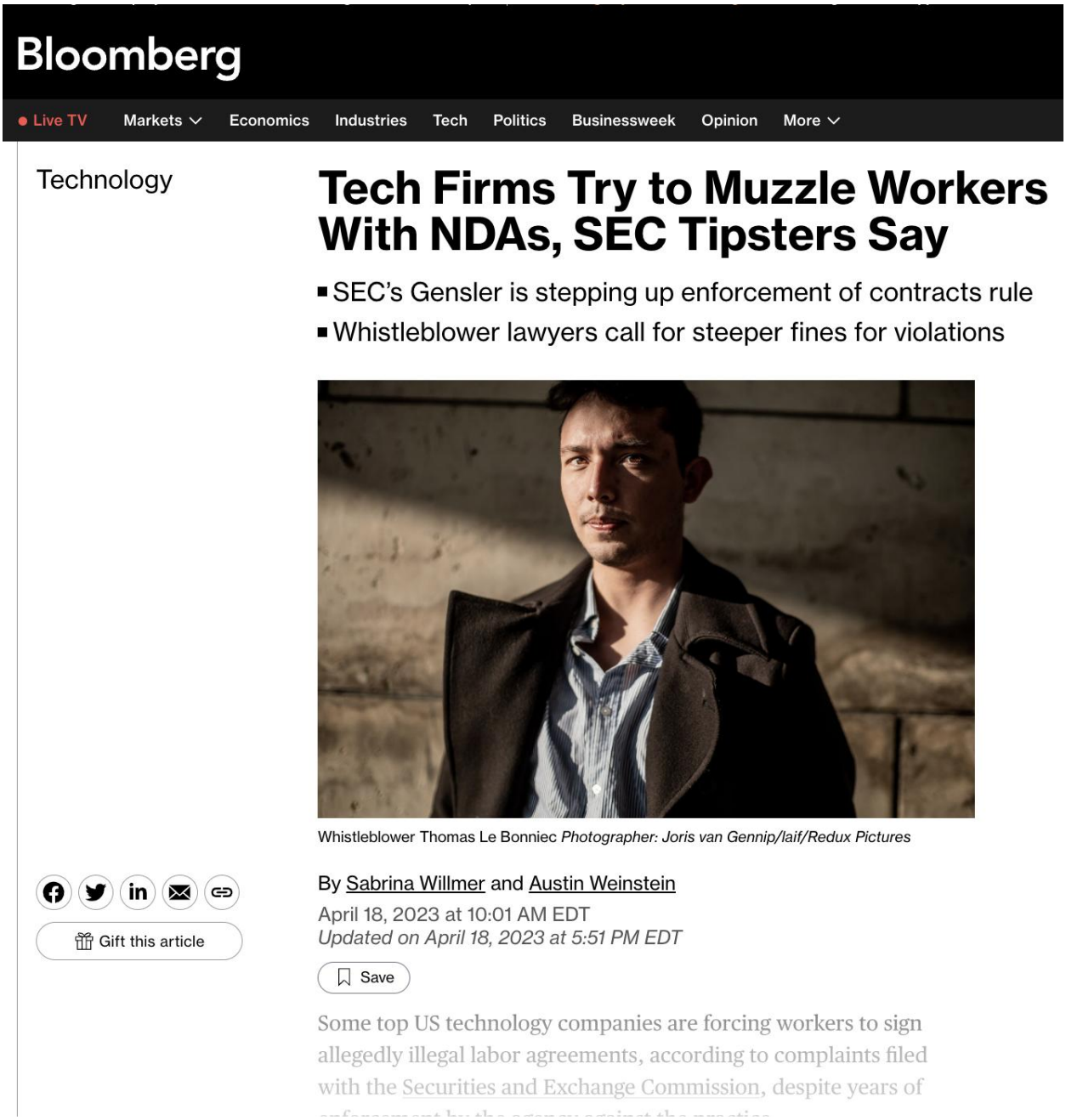
By: Thomas Le Bonniec

Title: Data Analyst

Dated: _____

Exhibit A

EXHIBIT B: 2023 BLOOMBERG INTERVIEW



Bloomberg

Live TV Markets Economics Industries Tech Politics Businessweek Opinion More

Technology

Tech Firms Try to Muzzle Workers With NDAs, SEC Tipsters Say

- SEC's Gensler is stepping up enforcement of contracts rule
- Whistleblower lawyers call for steeper fines for violations

Whistleblower Thomas Le Bonniec *Photographer: Joris van Gennip/laif/Redux Pictures*

Gift this article

By Sabrina Willmer and Austin Weinstein

April 18, 2023 at 10:01 AM EDT

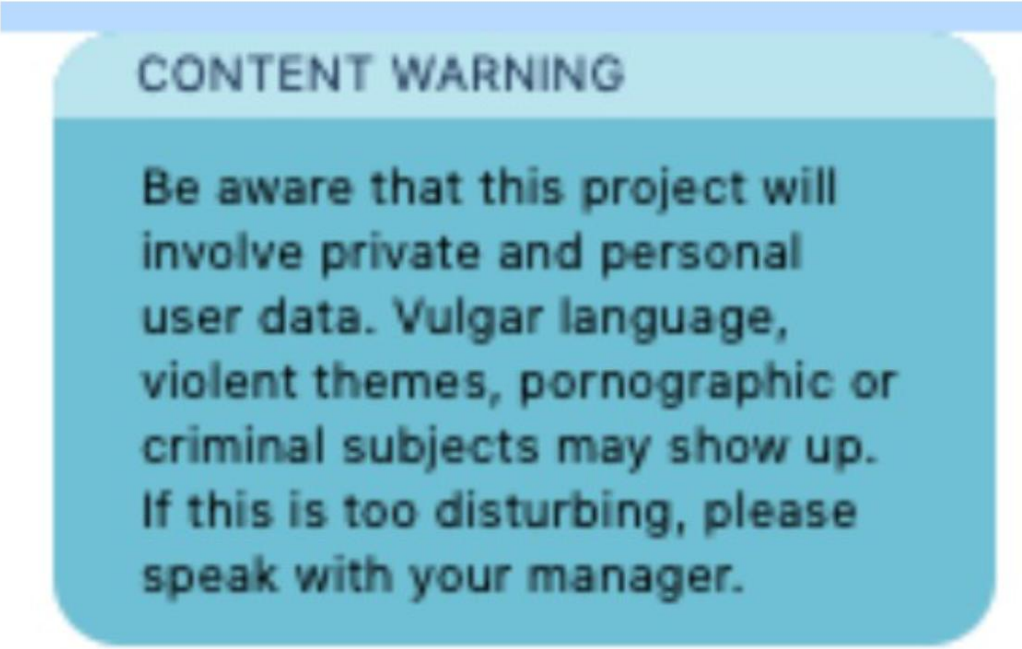
Updated on April 18, 2023 at 5:51 PM EDT

Save

Some top US technology companies are forcing workers to sign allegedly illegal labor agreements, according to complaints filed with the Securities and Exchange Commission, despite years of

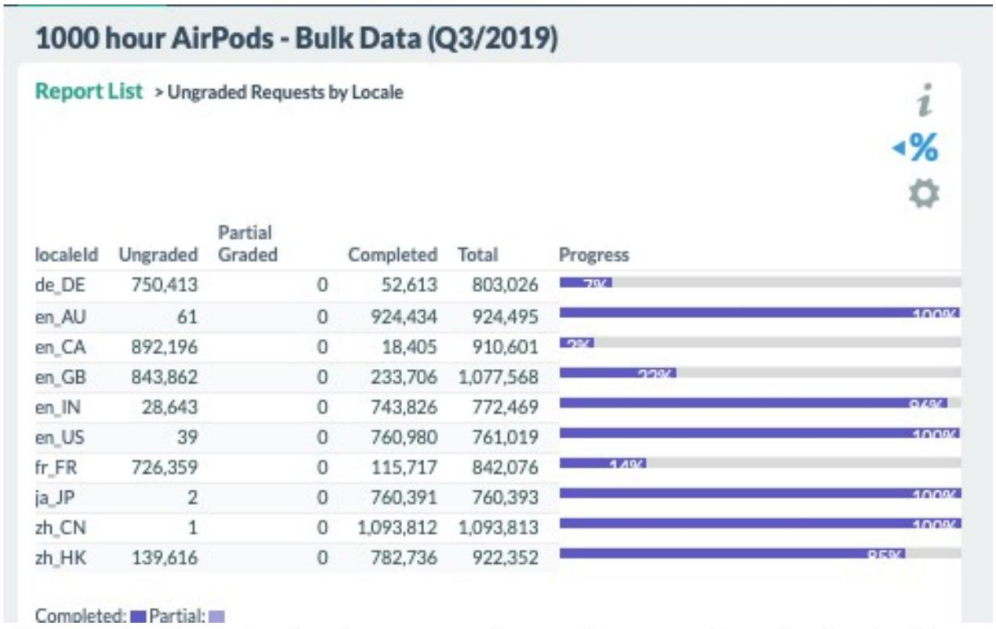
https://www.bloomberg.com/news/articles/2023-04-18/tech-firms-try-to-muzzle-workers-with-ndas-sec-tipsters-say

EXHIBIT C: SCREENSHOT OF SIRI GRADING PER COUNTRY



Capture 4: Warning label destined to "Data Analysts", before the guidelines

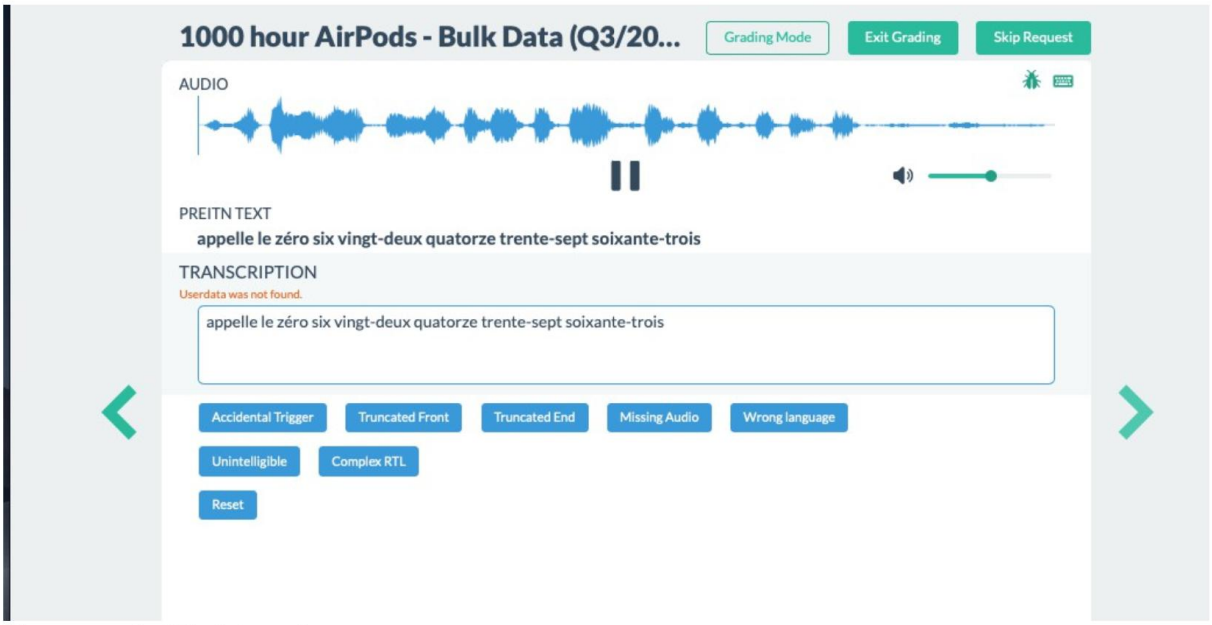
EXHIBIT D: SCREENSHOT OF SIRI GRADING PER COUNTRY



Capture 2 : Statistics for the corrected recordings on Airpods, for the 3ème Trimester of 2019

EXHIBIT E: SCREENSHOT OF SIRI RECORDING ON CROWDCOLLECT

The following are screen captures [107] made between late june 2019 and early july 2019 by the employee (Thomas Le Bonniec).
They describe the work effectuated in the context of the employment contract with the subcontractor (GlobeTech) and for the client (Apple).



Capture n.1: Work interface

Capture n. 1 illustrates the work interface and the task required to be done.

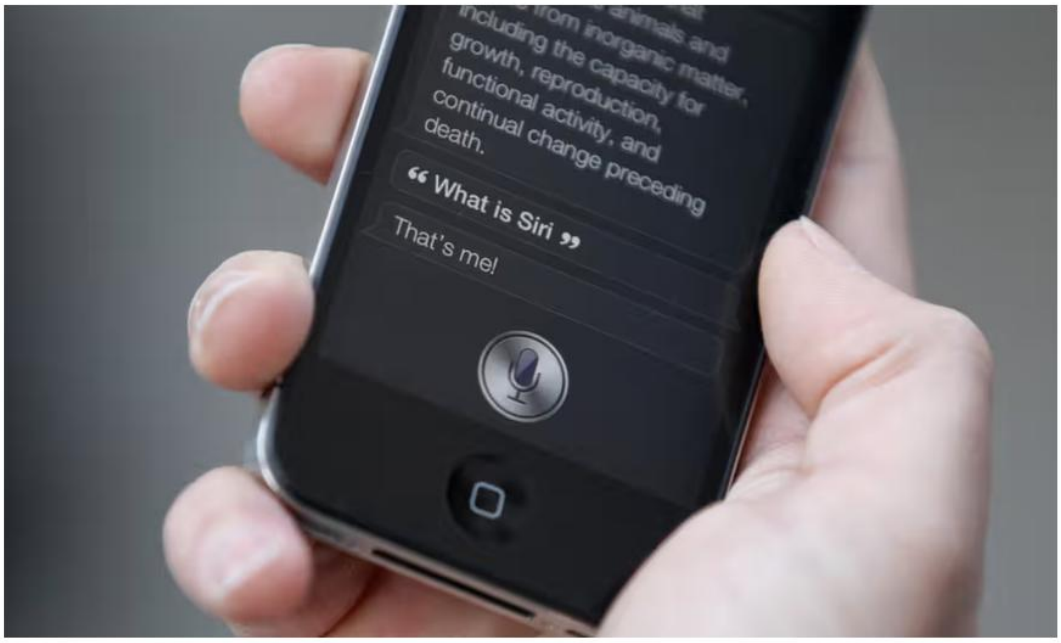
EXHIBIT F: 2019 THE GUARDIAN ARTICLE

Apple

This article is more than **4 years old**

Apple contractors 'regularly hear confidential details' on Siri recordings

Workers hear drug deals, medical details and people having sex, says whistleblower



Workers heard the information when or providing quality control for Apple's Siri voice assistant. Photograph: Oli Scarff/Getty Images

Alex Hern

Fri 26 Jul 2019 12.34 EDT

Apple contractors regularly hear confidential medical information, drug deals, and recordings of couples having sex, as part of their job providing quality control, or “grading”, the company’s Siri voice assistant, the Guardian has learned.

Although Apple does not explicitly disclose it in its consumer-facing privacy documentation, a small proportion of Siri recordings are passed on to contractors working for the company around the world. They are tasked with grading the responses on a variety of factors, including

https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings

EXHIBIT G: 2019 EL PAIS ARTICLE

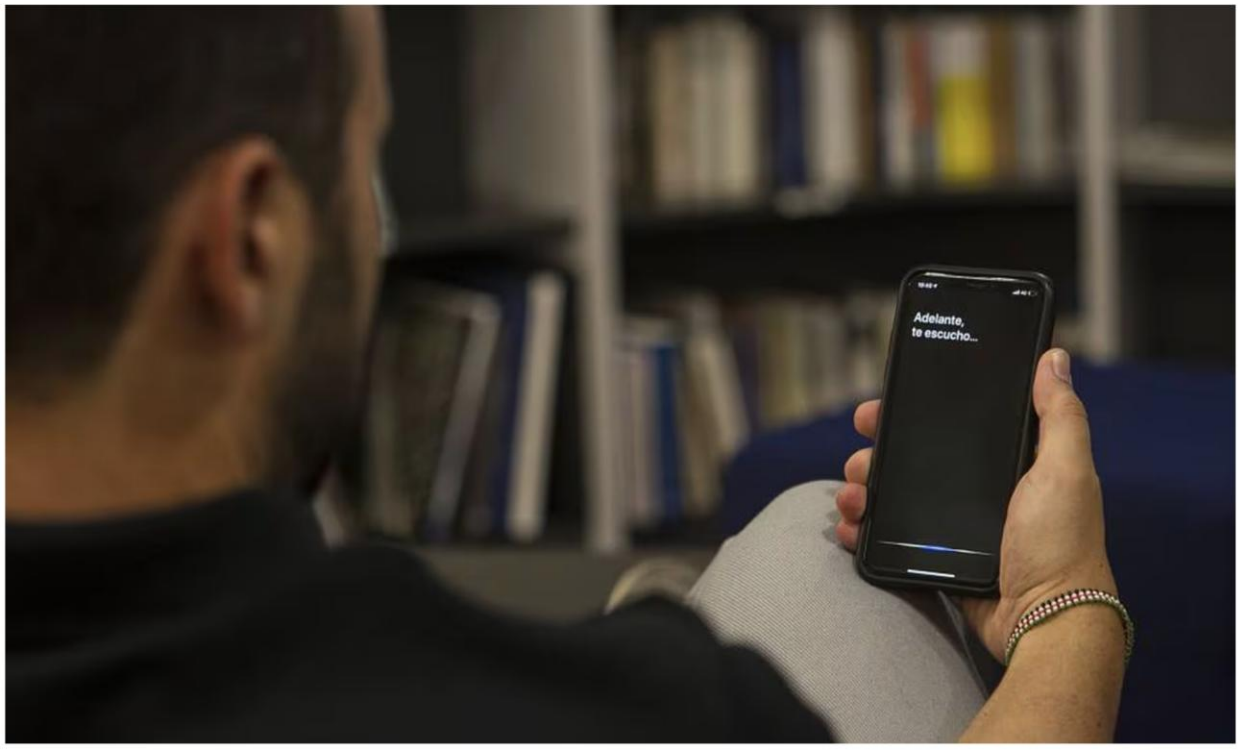
EL PAÍS SUSCRÍBETE

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIMAS N

Apple también contrata a personas para escuchar conversaciones privadas

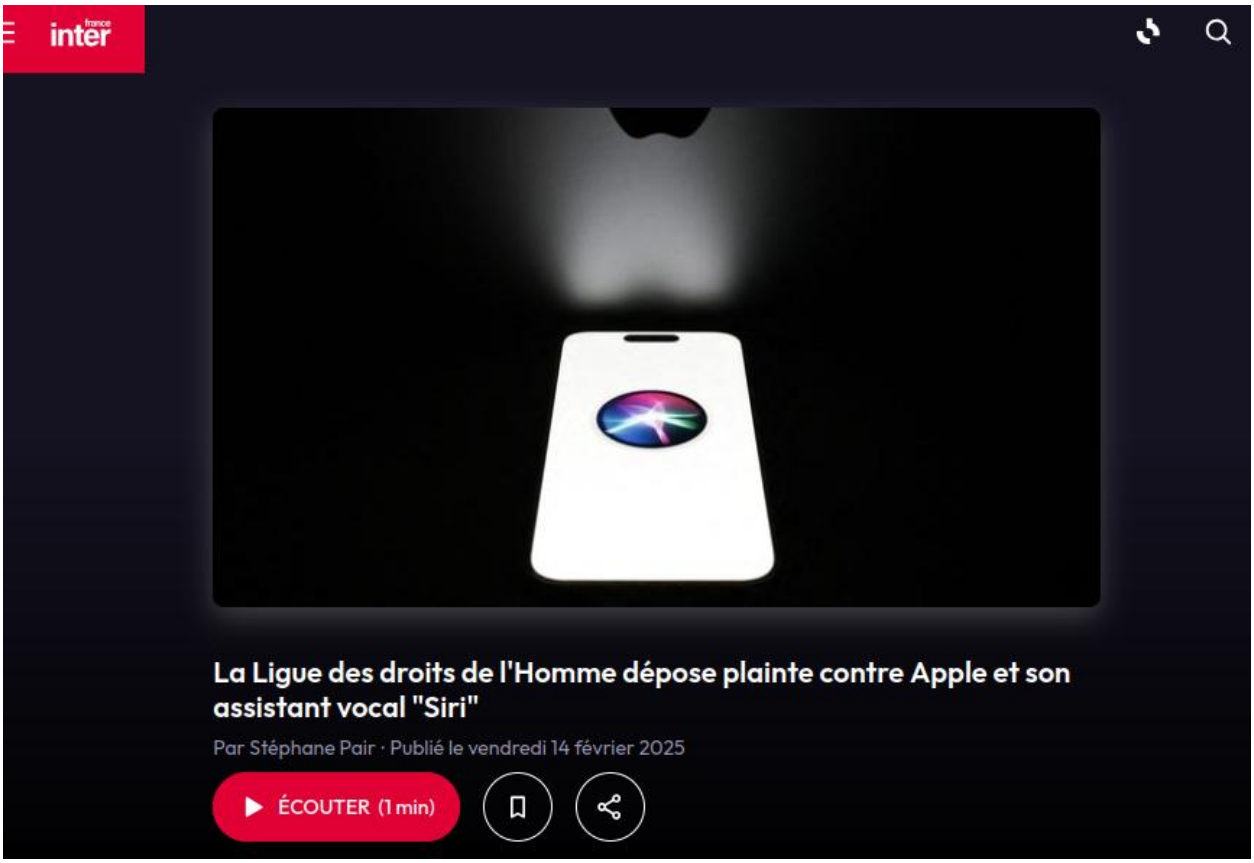
La compañía de Cupertino tiene transcriptores en España que revisan las interacciones de sus usuarios, incluidas las íntimas, en varios idiomas para mejorar el rendimiento de Siri



Un usuario realiza una consulta a Siri desde un iPhone.
JULIÁN ROJAS

https://elpais.com/tecnologia/2019/07/23/actualidad/1563902000_568286.html

EXHIBIT H : 2025 RADIO FRANCE ARTICLE



https://www.radiofrance.fr/franceinter/podcasts/l-info-de-france-inter/l-info-de-france-inter-3297121