WORKPLACE PRIVACY AFTER COVID-19

Digital Rights Program

August 13, 2020

PUBLICCITIZEN

ACKNOWLEDGMENTS

This report was written by Burcu Kilic, director of Public Citizen's Digital Rights Program, with assistance from Scott Hulver, intern in the Digital Rights Program. It has greatly benefited from comments provided by Robert Weissman, Peter Maybarduk, Jane Chung and expert editing skills of David Rosen.

Special thanks to Bret Thompson and James Smathers for their assistance with layout and graphic design.

ABOUT PUBLIC CITIZEN

Public Citizen is a national non-profit organization with more than 500,000 members and supporters. We represent consumer interests through lobbying, litigation, administrative advocacy, research, and public education on a broad range of issues including consumer rights in the marketplace, product safety, financial regulation, worker safety, safe and affordable health care, campaign finance reform and government ethics, fair trade, climate change, and corporate and government accountability.

Contact Public Citizen

Main Office
1600 20th Street NW
Washington, D.C. 20009

Phone: 202-588-1000

Capitol Hill
215 Pennsylvania Avenue SE, #3
Washington, D.C. 20003

Phone: 202-546-4996

Texas Office
309 E 11th Street, Suite 2
Austin, Texas 78701

Phone: 512 477-1155

For more information, please visit www.citizen.org.

TABLE OF CONTENTS

WORKPLACE PRIVACY AFTER COVID-19

The workplace is "where invasive technologies are normalized among captive populations of employees."

- Shoshana Zuboff, The Age of Surveillance Capitalism

Introduction

COVID-19 dramatically has changed how we think about the workplace. As businesses reopen and workers return, the spread of the coronavirus (COVID-19) is a serious concern. Amid the unrelenting first wave of infections and the prospect of recurring future waves, employers have been turning to new technologies to mitigate the risks – introducing a vast array of apps, wearables and other technologies. In a work setting, where activities are governed by a contractual or power relationship, many workers either must accept the new high-tech workplace surveillance or risk losing their jobs.

Without sufficient government regulation and guidelines, employers using these technologies are invading workers' privacy to varying degrees. Some technologies may place various worker rights in jeopardy, including the right to equal treatment, by:

- Tracking, monitoring, collecting and sharing personal data, including sensitive health data;
- Directly sharing data with employers, bypassing worker consent; and
- Posing increased cybersecurity risks.

The speed at which these new technologies have been deployed is concerning. Fifty new apps and technologies have been released since the pandemic began, not accounting for existing, unchanged technologies that now are being marketed as workplace surveillance tools to combat COVID-19. On June 16 alone, both Fitbit and Amazon released new workplace surveillance tools. From an employer's perspective, this rapid deployment is driven mainly by the urge to bring workers back to the workplace. But the invasion of privacy that workers face is alarming, especially considering that the effectiveness of these technologies in mitigating the spread of COVID-19 has not yet been established.

The default setting of most workplace surveillance apps is "mass surveillance by default." For instance, Microsoft and UnitedHealth Group's ProtectWell app sends COVID-19 diagnostic test results directly to the employer, bypassing the worker. Other apps don't treat workers' data as being subject to the requirements of the Health Insurance Portability and Accountability Act (HIPAA), meaning the data does not have to be securely handled and protected in accordance with HIPAA's health information privacy provisions. Some wearables are tracking employees' locations to identify and encourage behaviors. For example, if a worker has not spent enough time close to a sink, the app will identify them as likely not having spent enough time washing their hands.

The default setting of most workplace surveillance apps is "mass surveillance by default."

This report identifies nearly 50 apps and technologies being introduced into the workplace. COVID-19 health tracking technology currently is being used by at least 32 employers[1] to track at least 340,000 workers[2] and is available to up to 14,000[3] additional employers and almost 4 million workers[4]. The report describes what the apps are and how they work, highlighting specific privacy concerns. It concludes with a checklist of best practices for employers as they consider whether to introduce surveillance technologies into their workplaces.

[1] We have identified 32 employers that have either self-reported or identified in the news as adopting these technologies.

[2] 340,000+ workers is an estimate based on how the company is rolling out the technology (office v. manufacturing plant, a particular location, etc.). In the absence of any information about who would be using it or how many workers would be tracked, we estimated based on the kind of technology and workforce size.

[3] Many companies have released technologies embedded within existing systems and made these updates free to customers. We calculated the employers that could be using these technologies based on which businesses are existing customers and would have access to these updates.

[4] Based on how many employers had access to these free updates, we calculated the size of their workforce, estimating employees using the existing technology. This number, although it could be lower, is likely significantly higher as our customer and workforce estimates were conservative.

How Do Workplace-Surveillance Technologies Threaten Workers' Privacy?

Listed below are three apps being introduced into the workplace that invade workers' privacy. For each product, workers download the app onto their mobile phones and periodically fill out a survey of self-reported medical information, such as COVID-19 symptoms and temperature. Employers can access workers' information through a reporting platform, which allows employers to view self-reported medical information and identify workers who could have been exposed to other sick workers.

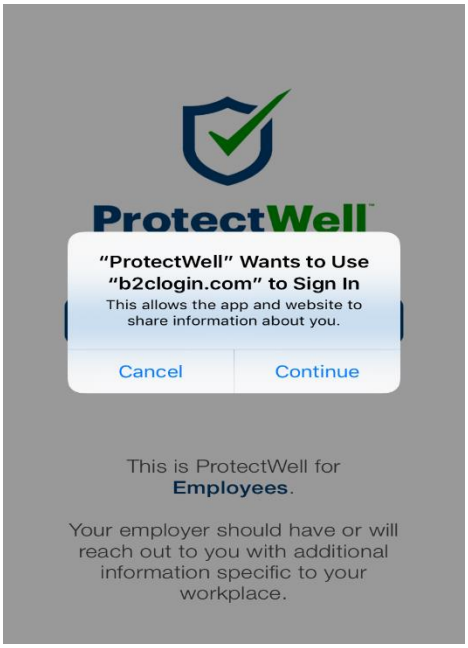
Here are some of their most alarming privacy-violating features, as described by their makers:

ProtectWell by Microsoft and United Health

- "Employers can direct their workers to a streamlined COVID-19 testing process that enables closed-loop ordering and **reporting of test results directly back to employers.**"
  - Microsoft Press Release

- "Any information disclosed to us in connection with the Site and the ProtectWell App **is not protected health information**, as defined under the Health Insurance Portability and Accountability Act of 1996 ('HIPAA')..."
  - ProtectWell Privacy Policy

- "We may **obtain additional information about you from third parties** such as marketers, partners, researchers, and others. We may **combine information** that we collect from you with information about you that we obtain from such third parties and information derived from any other subscription, product, or service we provide."
  - ProtectWell Privacy Policy



Healthcheck by Stratum

- "Our **workers and agents may view your Personal Information…**"
  - Healthcheck Privacy Policy
- "If you are accessing on a mobile device, we will **automatically collect personal data including device, content and usage data**… We also collect IP address access location to **determine your current location**…"
  - Healthcheck Privacy Policy

COVID-19 Worker Safety and Business Continuity Tracker by Pegasystems

- Your **personal information may be transferred, processed and stored outside the country where your information was collected** by using or attending a Service..."
  - Pegasystems Privacy Notice

Overview of COVID-19 Workplace-Surveillance Technologies

Table 1: Apps in which Workers Self-report Health Information

App	How it works	Who's Using it?
Pegasystems	Tool for employers to build custom COVID-19 symptom survey apps; data is aggregated in a central dashboard for the employer.	Unclear; introduced as part of an existing platform, to which these 60 companies have access
Back to Work (Cordata)	Workers fill out a pre-set survey embedded in the existing app; data is aggregated in a central dashboard.	Unclear; embedded in a platform used by 100+ companies
Arcoro	Worker survey built into existing time clock app; data stored on the cloud.	Titan roofing, a small business in Massachusetts
Workforce Safety (Appian)	Tool for employers to build custom COVID-19 symptom survey apps; data is aggregated in a central dashboard for the employer.	Unclear; separate app from what current customers use
Landing AI	Camera monitoring system to identify people who are not socially distanced.	Undisclosed
ProtectWell (Microsoft & United Health)	Tool for employers to build custom COVID-19 symptom survey apps; data is aggregated in a central dashboard for the employer.	United Health is rolling it out for their workers; Microsoft planning to use

HealthChampion	COVID-19 symptom survey embedded in existing app, data is aggregated in a central dashboard.	Undisclosed
Work.com (Salesforce)	Tool for employers to build custom COVID-19 symptom survey apps & contact tracing; data is aggregated in a central dashboard for the employer.	Undisclosed
Check-In (PwC)	Workers submit health status; app also has automatic contact tracing.	PwC will use internally; unclear who else
Check-In Online	Digital form to gather information from employees, visitors, automatically process the information and complete simple calculations.	Canon
HealthCheck (Stratum)	Workers fill out a pre-set survey; data is aggregated in a central dashboard.	"Several Wall Street banks and retail and insurance companies have signed on or are in talks to use HealthCheck"
Dayforce Worker Safety Monitoring (Ceridian)	Managers can pull up reports and draw insights based on workers' self-reported data.	Undisclosed
SafetyTek	Helps managers in workplace settings track the health of their personnel with an easy-to-follow COVID-19 self-assessment tool.	Undisclosed
Agility (Net Health)	COVID-19 tracking embedded in existing platform that focuses on exposure tracking among medical frontrunners.	Undisclosed
COVID19Tracker (Kokomo24/7)	AI-powered scoring system designed to manage false positives and pinpoint at-risk workers more accurately.	Undisclosed
Mayo Clinic	Uses the clinic's electronic health records to help notify any staff members that may have been exposed to a patient or staff member who's tested positive.	Rochester, Florida, and Arizona Mayo Clinic campuses
Emocha	Workers fill out a pre-set survey; data is aggregated in a central dashboard.	Five hospitals in Baltimore area and Johns Hopkins
PRA Health Sciences	Workers fill out symptom survey; employers tag workers with one of three severity categories.	"in discussions with academic institutions, governmental organizations, health departments and other private businesses"
Health Check (Harri)	Screens workers for symptoms; data aggregated in a central dashboard.	Kapow Noodle Bar
Social Safety App (FROM)	Uses Bluetooth to give a warning if too close to another worker.	Not yet released, preparing for private beta-testing
WellnessCheck (Pinpoint Health)	App or website screens workers for symptoms; data aggregated in a central dashboard.	Undisclosed

SaferMe	Symptom survey coupled with geo-tracking for employers to manage.	Lists customers but unclear for which product; CEO quoted saying 10,000s were using it, just signed with Fortune 500 company
Back on Track (Ferrari)	Health symptoms uploaded through app, contact tracing enabled.	Maranello and Modena offices

Table 2: Wearables Tracking Workers' Locations

App	How it works	Who's Using it?
AiRSTA Flow	Bracelets use Bluetooth to track interactions.	In talks with hundreds of companies, and historically a big set of clients has been prisons
Blackline Safety	Wearables plus an app used for contact tracing.	Emergency response business
CarePredict	Wearables track location and time of contact in a centralized dashboard for nursing home staff and residents.	Several nursing homes, e.g. the Legacy at Town Square in Austin, TX
CenTrak	Radio-frequency identification (RFID)-enabled lanyards worn by workers provide time and location data to track if workers are taking health precautions (e.g. washing their hands).	Already installed in 1,700+ facilities
Estimote	GPS location tracking and Bluetooth contact tracing; collected information is centrally stored and displayed on a health dashboard that "provides detailed logs of possible contacts."	Unclear, but past clients of the company include Amazon, Apple and Nike
Ready for Work (Fitbit)	Wearable feeds health information into app along with self-reported symptom information for employers to decide who is cleared for work.	Undisclosed
Rombit	Bracelets beep if not social distancing.	Belgian ports (thousands of workers)
PointGrab	Cameras and sensors track distance between people and whether good hygiene is being practiced .	Companies including Philips and Mitsubishi
Proximity Trace (Triax)	Wristbands notify wearer if within 6 feet of another worker and track contact for exposure tracing.	Undisclosed
Safezone	Wristbands notify workers if they're too close together and give contract tracing notifications.	New York Knicks, Chicago Bulls, Paris St Germain; Eintracht Frankfurst (Bundesliga); "major automotive manufacturer in Germany and a food manufacturer in the US"
TraceSafe	Bracelet with an embedded chip and related software to track the wearer's location.	Hong Kong immigration quarantine program; Toronto Wolfpack Stadium
TraceTag	Device of Proximity Trace is affixed to any hardhat or worn on the body for proximity detection and contact tracing. Workers interactions are	Gilbane Building Company

	logged for contact tracing in the event of a conformed COVID-19 case on site.	
Universal Contact Tracing (Microshare)	Workers wear wristbands or badges to track contact with other workers.	Many different settings, no specifics disclosed.

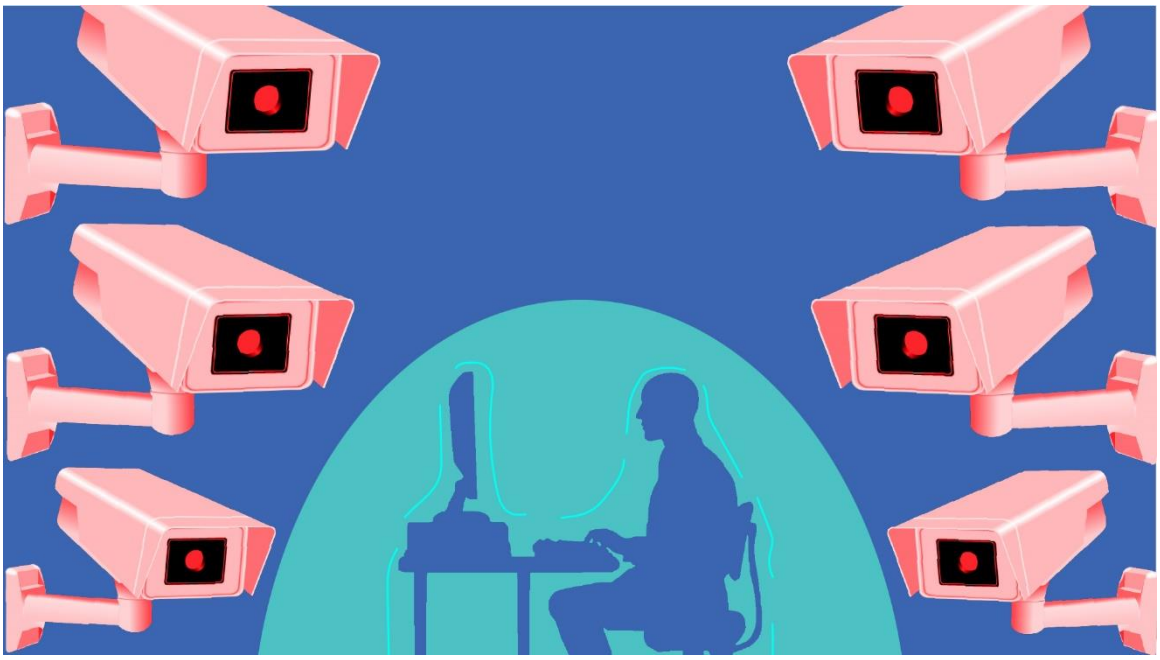
Table 3: Hardware (Cameras, Sensors, etc.) Tracking Workers' Locations

App	How it works	Who's Using it?
Distance Assistant (Amazon)	Camera feeds to monitor, showing a live stream of workers augmented by 6 foot circle, for workers to see if they are social distancing.	Will be made open source
Health Pass by CLEAR	Users need to upload personal health documents, including test results for COVID-19; upon entering office, users go through facial recognition scanning, take a real-time health quiz, and provide proof of their previous COVID-19 test by scanning a QR code.	In talks with restauranteur Danny Meyer (25 restaurants and Shake Shack) and New York Mets
KastleSafeSpaces	Touchless technology, integrating virus-screening and contact tracing processes.	Monday Properties (national real estate investment and development company)
MotionWorks Proximity (Zebra)	Proximity sensing with user-level alerting and contact tracing.	Zebra's own distribution centers in the Netherlands
NICE Alliance	Working to make cameras interoperable with capabilities for detecting social distancing, face mask use and temperature.	"Pushing for adoption by elevator management firms… discussion is underway with the city of Tel Aviv to monitor public transportation and schools" still in trial and will be rolled out to early adopters in the Fall[5]
Nodle M1	Device tracks distance and notifies workers with a buzz when they get too close to one another; supposedly more precise than smartphone-based solution, and without the need for location.	Says they have "received interest from large enterprises in the U.S. and Europe for several million units", but doesn't specify
Pop ID	Scans body temperature for those who want to enter; face payment for no contact transactions; replace key cards by automatically unlocking doors for workers whose faces are recognized.	CaliBurger (international restaurant chain with seven locations in the U.S.[6]); Subway franchise owners (about 50 restaurants); Lemonade (California restaurant chain); Taco Bell locations

[5] https://finance.yahoo.com/news/post-lockdown-smart-cameras-could-134549590.html

[6] https://findbiometrics.com/caliburger-uses-biometric-tech-guard-against-covid-19-032603/

Radiant RFID	Workers receive a vibration and a color-coded warning on the watch when they are closer than six feet to another person; supervisors also receive alerts and reports.	Ford factories
Sewio	Workplace-specific contact tracing using sensors and worker badges to track workers' locations.	21 companies around the world
Smartvid.io	Camera monitor social distancing and health practices (ex. wearing masks).	Unclear; introduced as part of software that these companies use
VergeSense	Wireless Sensor that measures distance between employees and interaction frequency, analyses data and produces daily social distancing report on social distancing.	Customers include Roche, Cisco, Shell, BP, Telus, Rapid7, JLL, Quicken Loans, Fresenius



BEST PRACTICES FOR EMPLOYERS CONSIDERING INTRODUCING WORKPLACE SURVEILLANCE

☐ Ask the Right Questions

- Gather as much information as you can to make an informed decision:
- How does the product work?
- What data is being collected?
- What is the purpose for such collection? Could you achieve the same results without collecting personal data?
- Where will the data be stored? Will it be stored on an individual's device or on a separate server?
- How long will the app keep the data? Is there any justification for the app to keep the data beyond 30 days?
- Will the data be shared with public health authorities?
- Does the developer have access to the data?
- Will the developer share personal data with third parties?

☐ Limit Data Collection to Essentials

Articulate why you need each functionality of the app and take steps to ensure that:

- Data collection is limited to what is truly necessary.
- A time frame is provided for how long collected data will be retained, and data is kept no longer than is needed.
- Access to and use of the data is restricted to authorized people and only for the appropriate amount of time.
- Restrictions are placed on third-party sharing of data.
- Data is not repurposed.

☐ Ensure Cyber Security

Promote the use of encryption, pseudonymization and anonymization where appropriate.

☐ Transparency & Disclosure

Be transparent with workers, creating formal practices to:

- Provide a privacy notice, inform employees about the type of data the app collects, how the data would be used, who has access to the data and when the data will be deleted.
- Establish open and transparent communication: encourage workers to voice concerns and ask questions.

☐ Worker Opt-In & Rights

Promote workers' rights by implementing policies that:

- Provide apps on a voluntary basis and seek informed consent of workers to secure their trust and confidence.
- Ensure workers have the right to access, correct and delete their information, withdraw their consent any time, have the right to receive an explanation when their data is used and challenge those uses if necessary.

☐ **Restrict Collection of Biometric Data**	Collection and processing of biometric data should only be considered as a last resort if there are no other less intrusive means available. It should be necessary and limited to the minimum required to achieve the purpose and be done only with full and informed consent, subject to clearly defined restrictions on collection, use, storage and destruction of that data.
☐ **Introduce Internal Policies & Procedures**	Create written internal policies and share them with workers, in order to: • Enforce tight controls to the data. • Clarify who has access to data. • Develop confidentiality guidelines, implement operating procedures. • Establish a designated point person for COVID-19-related privacy issues and procedures, who is trained to maintain worker privacy and confidentiality.

Before deploying these apps, employers should take caution to fully vet the technologies being used to ensure the utmost privacy and confidentiality at the workplace.

www.citizen.org