Best Practices for Employers Considering Workplace Surveillance

1 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?

2 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

3 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

PUBLICCITIZEN

PROTECT PRIVACY, COMPLETE THE CHECKLIST

4

Ensure Cyber Security

Promote the use of encryption, pseudonymization and anonymization where appropriate

5

Worker Opt-In & Rights

Be transparent with workers, creating formal practices to:

- Provide a privacy notice, inform workers 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

6

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 only be done with full and informed consent, subject to clearly defined restrictions on collection, use, storage and destruction of that data

7

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.

Read the Full Report at citizen.org