CovidCop19 – The rise of employee surveillance

28 January 2021

@AdvocateDVB

Topics

- The emerging landscape
- Ethics and thoughts
- The legal landscape

The Emerging Landscape

- Types of surveillance
  - Internet and app usage.
  - Keystrokes.
  - Email.
  - Computer screen recording.
  - Phone use.
  - Video/audio surveillance.
  - GPS tracking by vehicle.
  - Location tracking by access badge.
  - Body heat sensors.
  - Time recording.

The Emerging Landscape

- A recent study by academics at Cardiff University and the University of Southampton found that

“a common fear among bosses is that out-of-sight workers will "shirk” and productivity will fall.”.

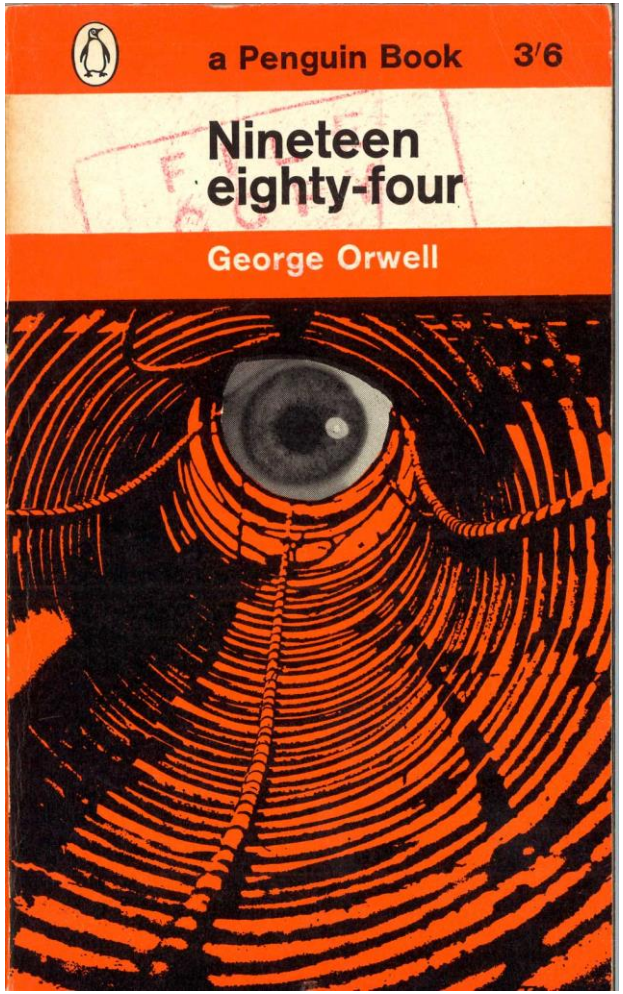
The Emerging Landscape

The Emerging Landscape

The Emerging Landscape

The Emerging Landscape

Ethics and thoughts



Thoughts

- CIPD produced a report on workplace technology and the employee experience:
- **Monitoring and surveillance**
  - 45% of employees believe that monitoring is currently taking place in their workplace.
  - 86% believe that workplace monitoring and surveillance will increase in the future.
  - 73% of employees feel that introducing workplace monitoring would damage trust between workers and their employers.
- **Employee voice**
  - Only 35% of employees and/or their representatives have been consulted on the introduction and/or implementation of new technology.

The Law

- Fairness, transparency and data minimisation
- Providing a clear and transparent notice on monitoring to employees. This should detail specifically why the monitoring is taking place and the particular nature and extent of the monitoring;
- Providing employees with details about how monitoring is conducted. This policy should also be displayed visibly in the workplace and be re-issued if monitoring activities change; and
- Choosing a method of monitoring which is not excessive, and which takes into account the reasonable privacy expectations of employees (where a less intrusive option to employee monitoring exists that will achieve the same results, the employer should opt for this).
- Care should be taken to avoid monitoring purely personal and non-professional data where its personal nature is clear from the outset, regardless of whether such data is stored on IT equipment belonging to the employer.

The Law

- Don’t forget – Art.16 of the Data Protection (Jersey) Law 2018

16 Data protection impact assessments required for high risk processing

(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, a controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before the processing, to be known as a data protection impact assessment.

(2) In assessing the risk to the rights and freedoms of natural persons, regard must be had in particular to the use of new technologies, and the nature, scope, context and purposes of the processing.

(5) A data protection impact assessment is, in particular, required in the case of –

(a) a systematic and extensive evaluation of personal aspects relating to natural persons that is based on automated processing, and on which decisions are based that produce legal effects concerning, or similarly significantly affecting, those persons.

(b) the processing of special category data on a large scale…

The Law

https://jerseyoic.org/media/joqfvcyo/16_tk_dpia-template_interactive.pdf

Data Protection Impact Assessment (DPIA) Template

This template is an example of how you can record your DPIA process and outcome.. You may also wish to refer to the guidance "Criteria for an acceptable DPIA" published by the European Data Protection Board (previously the Article 29 Working Party) guidelines on DPIAs.

You should start to fill out the template at the very start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

This template is intended to provide a starting point and should be amended, reordered, and/or added to as necessary and as appropriate for the controller's organisation and the nature and scope of the issues being considered as part of the DPIA.

Submitting controller details

Name of controller	Name of controller
Subject/title of DPO	Subject/title of DPO
Name of controller contact/DPO (delete as appropriate)	Name of controller contact /DPO

Executive summary

This section should record at a high level the key facts from the assessment as well as the conclusions drawn. The section should include:

- A high-level description of the proposed processing.
- A summary of the processing scope.
- A summary of the purposes for which processing will occur.
- A summary of the intended benefits for data subjects, third parties and the controller.
- A summary of the rationale as to why a DPIA is required.

If it goes wrong…