



## SUMMARY BY REGION

# Employee Monitoring Law: Then, Now and the Future

## Europe – key points

- The most stringent restrictions on employee monitoring arise from jurisdictions in Europe;
- Monitoring needs to be fair, transparent, proportionate and have a specified purpose;
- GDPR implements even stronger and more uniform requirements;
- Cases focus on how clear an employer's policy is, the business need for the monitoring, the proportionality in relation to the risk posed, and the severity of the conduct in question;
- There are varying approaches to admissibility of evidence improperly obtained by employers:
  - France has been more strict in excluding such evidence;
  - Belgium and the UK have been more lenient, provided the evidence is relevant to the proceedings and there is no public policy reason to exclude the evidence.
- There is an increased willingness by the European Court of Human Rights (ECtHR) to defend privacy rights in the context of the workplace. Respect for private life and correspondence continue to exist in the workplace, even if restricted so far as necessary.

## North America – key points

- The US has no comprehensive federal privacy regime, but there are pockets of legislation (for example, relating to health data), and more liberal states have introduced regulations. Additionally, in relation to EU data subjects, the US must comply with the Privacy Shield Framework.
- The National Labor Relations Board (NLRB) has taken the position that employee's negative comments about the workplace may be protected under 'concerted activity' speech, including when it is on social media. This employee protection is beyond that which has been permitted in most other countries around the world.
- All US states (except for Alabama and South Dakota) have adopted data security breach notification laws, implying that levels of monitoring should allow for adequate incident response.
- More states are increasingly (currently 30) prohibiting inquiries into a potential employee's criminal convictions prior to an offer of employment being extended.
- Canada has detailed federal legislation in relation to the protection of personal information in trade and commercial activities. This incorporates ten principles in relation to the collection, use, retention, disclosure and access to personal information.
- Canada appears to have applied the law relating to monitoring and surveillance in a similar way to the courts in Europe. A balance should be struck between addressing a specific monitoring need with the loss of privacy involved.
- A residual expectation of privacy remains when monitoring IT in the workplace.

## Other jurisdictions

Australia, the Middle East, Singapore, Brazil and India are covered in their individual reports as it difficult to generalise in terms of the regions they sit within given the necessarily limited scope of this report.

Please see the main report for further detail, surrounding context and case information relating to all of the above key points.

Organisations must be aware that legal considerations for employee monitoring will vary from organisation to organisation and specific issues will arise depending on the nature of the organisation undertaking monitoring and the risks it is trying to mitigate. Dentons UK and Middle East LLP (Dentons) prepared a report for NPSA on Employee IT Monitoring in March 2018 (the Report), to serve as a legal resource only, it is not a substitute for professional advice. These documents provide a snapshot of some of the information contained in the full Report and must not be read in isolation. Neither the Report nor these documents are designed to provide legal or other advice and you should not take, or refrain from taking, action based on their content. The Report and the documents are not a comprehensive report of all the information or materials that are relevant to this area of law, and do not address any particular concerns, interests, value drivers or specific issues you may have. This is a complex area of law that is changing rapidly. If you require assistance with a specific issue, you should seek legal advice from an appropriately qualified professional. Organisations planning to implement or review existing employee monitoring should seek their own professional advice. The Report (and therefore the information contained in these documents) was current as of the date of the Report publication (being March 2018). Neither NPSA nor Dentons owe any duty to you to update the content of the Report or these documents at any time for any reason. Please note the Report and these documents do not represent the views of NPSA or Dentons. Neither NPSA nor Dentons UK and Middle East LLP accept any

responsibility for any loss which may arise from reliance on the Report and/or these documents.

### Freedom of Information Act (FOIA)

This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

### Disclaimer

This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2018