CPNI
Centre for the Protection of National Infrastructure

大成 DENTONS

India: Relevant legislation

We have identified the following key pieces of legislation which are applicable to employee IT monitoring in India. Note that there is other legislation which is applicable which we have not included in this document.

Constitution of India

- Right to freedom of speech and expression (e.g. when a person is talking on the phone)
- This protects the right to privacy as part of the right to life and personal liberty. Currently this is enforceable only against State actors; however, the Supreme Court has recommended the Government formulate a data protection regime safeguarding against dangers to privacy from non state actors.

Information Technology Act 2000 (IT Act) and The Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules)

- Provides for compensation for negligence by a corporate body handling sensitive personal data or information (SPDI) in implementing 'reasonable security practices and procedures';
- Organisations should have privacy and disclosure policies, and software monitoring programmes to prevent unauthorised use or access to SPDI;
- Employee surveillance must have the informed consent of employees. It is advisable to obtain written consent from employees prior to using any monitoring software (consider inadvertent discovery of SPDI during an investigation).
- Employers are required to implement security procedures in line with ISO standards;
- Employee devices should only monitor workplace-related communication and should not intercept any other kind of information.
- The IT Act prescribes a criminal penalty for any person who secures access to electronic records without consent.

Indian Telegraph Act 1885 read with Indian Telegraph Rules 1951

- Permits interception of messages as directed by government officers, but unauthorised surveillance of telephone or mobile phone conversations may amount to a statutory violation in addition to violating the right to privacy.
- Messages, however, may be produced as evidence of criminal conduct by employees. Under current jurisprudence, tape-recorded conversations, even if obtained illegally, may be used in criminal trials.

Principles deduced from case law

Key principles to consider when judging the validity of any rule or policy which allows the collection of personal data include whether there was:

- notice given to the employee;
- The requirement for informed and individualised consent of the employee;
- a limited purpose for which data may be collected, used and retained;
- fair, just and reasonable monitoring;
- a legitimate aim/need; and
- a risk that was proportionate to the monitoring undertaken.
- Case law indicates that courts may be hesitant to interfere where employees have expressly consented to the company's collection and sharing of their personal information via a privacy policy in a private contract.

The future

GDPR: India is not currently recognised as providing adequate protection of personal data as defined by GDPR. This means that additional safeguards may need to be in place in order for organisations to transmit personal data from India to the EU. Indian companies that collect personal data from EU citizens and companies with established operations in the EU should consider whether their operations fall within the scope of the GDPR and, if so, the steps that need to be taken to achieve compliance with its requirements.

Data Protection Bill 2017 (not yet enacted)

- Provides for collection and disclosure of personal information subject to express and informed consent, for the purpose of performing a contract or the employer's legitimate interests.
- The Bill expressly bars surveillance by private corporate bodies.
- Bars profiling or harassment based on personal data. This has legal implications for any employer-installed software (e.g. AI) programmes seeking to profile employees.

White Paper on Data Protection in India 2017

The Committee emphasized the importance of freely given, informed and specific consent to the processing of personal data by way of a well-designed notice.

CPNI
Centre for the Protection of National Infrastructure

大成 DENTONS

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 CPNI on Employee IT Monitoring in March 2018 (the Report), to serve as a legal resource only, it is not a substitute for professional advice. This document provides a snapshot of some of the information contained in the Report and must not be read in isolation. Neither the Report nor this document 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 this document 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 this document) was current as of the date of the Report publication (being March 2018). Neither CPNI nor Dentons owe any duty to you to update the content of the Report or this document at any time for any reason. Please note the Report and this document do not represent the views of CPNI or Dentons. Neither CPNI nor Dentons UK and Middle East LLP accept any responsibility for any loss which may arise from reliance on the Report and/or this document.

© Crown copyright 2018