Where are the limits of monitoring communications if you suspect misconduct, e.g. Hotmail/Gmail, Instagram/Facebook on work devices or work email access on personal devices?

White Paper Conference

Catherine Taylor
CMS CMNO LLP

I always feel like someone is watching me… I have no privacy

The legal context

- Data protection rights
- Electronic monitoring protection
- Rights of privacy
- Trust and confidence
- Risk of claims

Data protection considerations

Before monitoring can take place, employers should:

- Establish the lawful basis for processing the data – IT use and social media policy
- Carry out a data protection impact assessment (DPIA)
- Transparency is key - ensure that the employee has been given notice that the monitoring may be carried out
- Ensure your Employee Privacy Notice/BYOD policy is fit for purpose

Statutory regulation of communications

- **Investigatory Powers Act 2016** and the **Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018**
- It is an offence under the IPA 2016 to intercept a communication unless the activity falls within an exemption. **One exemption is lawful authority**
- The Monitoring Regulations provide the routes for relying on lawful authority. This can be
  - with consent of those involved, (but includes consent of sender and recipient, so difficult for external communications)
  - without consent – which is likely to be more relevant for employers
- There is a lengthy list of reasons why businesses can monitor without consent – this includes "*establishing whether company staff, who are using the relevant telecommunications system are achieving the standards required by their company in the course of their duties*"
- In order to rely on this exemption the employer must make all reasonable efforts to inform the employees that the interception will take place – i.e. have a policy in place

Is there a right to privacy?

- Employees have a human right to a private and family life, both in and out of the workplace (Article 8, European Convention of Human Rights)
- Private sector employees will most likely link a claim based on their privacy rights to another claim e.g. unfair dismissal
- In UK monitoring cases alleging breach of A.8, relevant factors include:
  - Whether the employee had a reasonable expectation of privacy
  - Whether the IT policy explained monitoring would happen
  - If misconduct is alleged then the employee is considered to be on notice of an investigation and possible monitoring
  - Balancing of an employer's other obligations, e.g. the health and welfare of others
- *Barbulescu v Romania* – employer's monitoring of the personal use of Yahoo messenger amounted to a breach of right to privacy – "*an employer's instructions cannot reduce private social life in the workplace to zero.*"

Brake & another v Guy & others (2022)

- Claimants former owners of business acquired by defendant and now employees
- Alleged misuse of private information and breach of confidence when defendant accessed personal emails sent by claimants from business general ‘enquiries’ account
- Court of Appeal upheld finding that no reasonable expectation of privacy and no right of confidentiality in respect of those emails sent and received using business account
- Followed *Bloomberg LP v ZXC* to reinforce the fact specific nature of the enquiry
- Confirmed burden is on claimants to show reasonable expectation of privacy – facts in this case did not support that
- Also said that where there was misconduct this was a factor which could be taken into account in considering the expectation of privacy

Trust and confidence

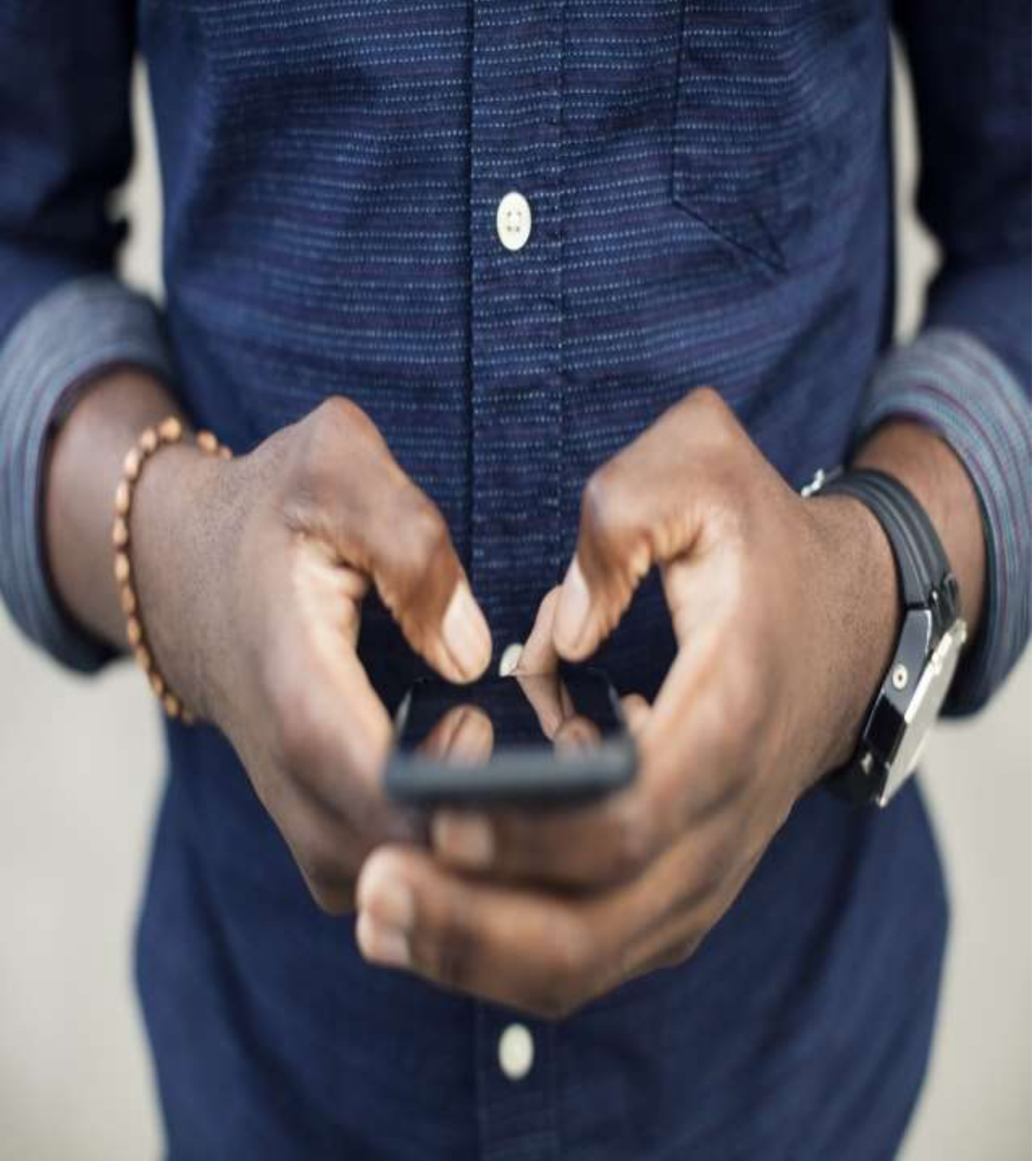
- The implied term of trust and confidence is a **mutual obligation** applying to both employers and employees
- Excessive or unwarranted monitoring by the employer may breach this term
- If the breach is sufficiently serious an employee may claim **constructive dismissal**
- If successful, in addition to compensation, the employee is released from their post-termination restrictions (e.g. non-competes)

Risk of claims

- Possible an employee will counterclaim based on stand alone data protection or other rights relating to monitoring – e.g. *Brake*
- The employee could also bring a claim for constructive dismissal – most relevant in employee competition situations
- Most likely claims are that the monitoring impacts the fairness of dismissal and/or is discriminatory:
  - Substantive fairness - The unfair dismissal legislation must be read and given effect so as to be compatible with Article 8 HRA
  - Procedural fairness - A reasonable investigation may be rendered unreasonable if the employee's data protection rights, right to privacy etc are disregarded
  - Discrimination – difference in treatment/detrimental treatment may leave the employer vulnerable

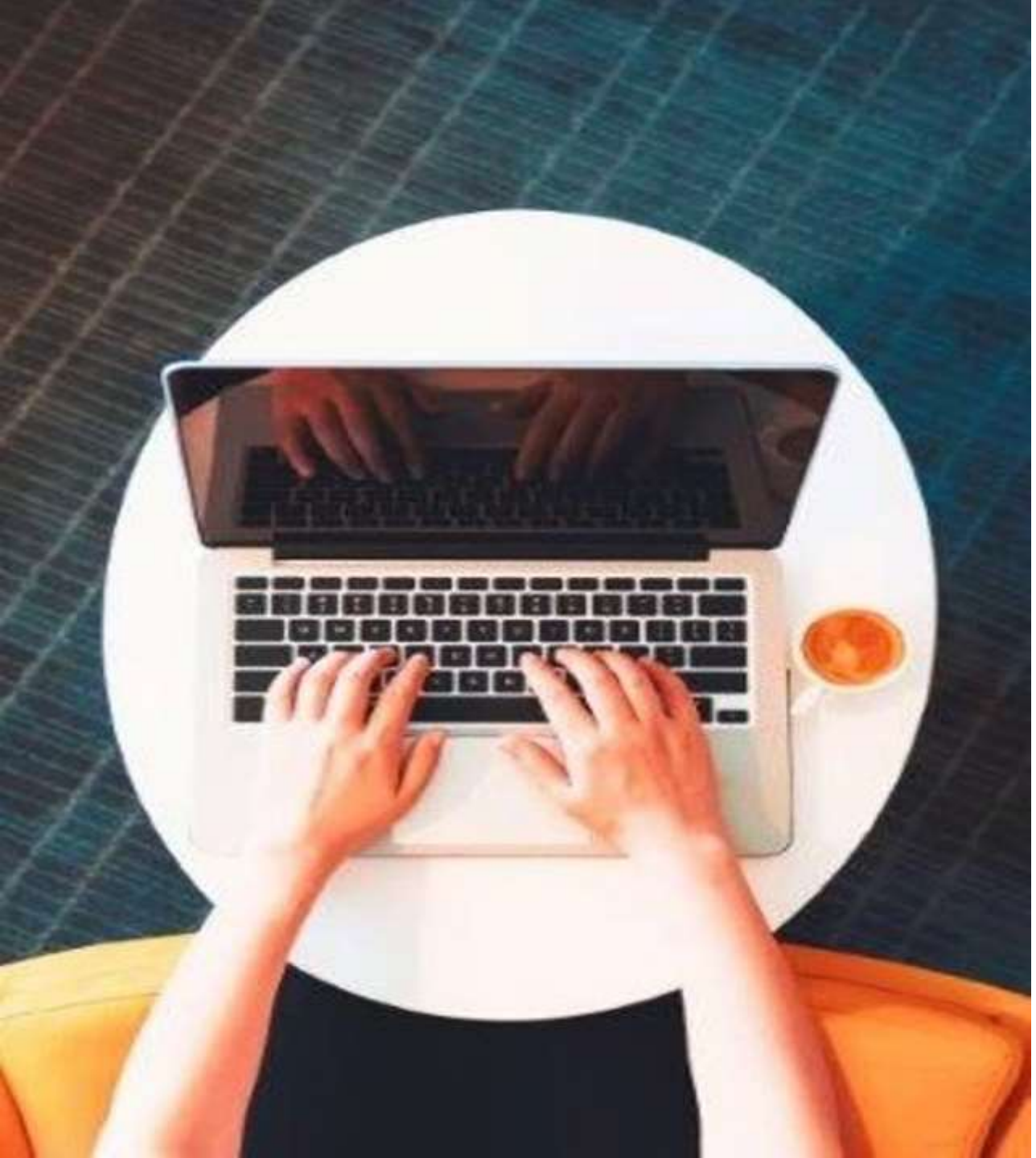
Garamukanwa v UK (2019)

- Claimant an employee accused of harassment by a colleague
- Alleged misuse of private information and breach of confidence when employer used evidence provided by the police after criminal complaint investigated
- European Court of Human Rights found the dismissal was fair:
  - No right to privacy engaged – this was lost after the initial complaint of harassment in relation to evidence relating to that complaint
  - Even if there was a right of privacy, it was proportionate for the employer to interfere with it to protect the health and welfare of others
  - But…fact specific investigation as to whether privacy was engaged



Limits on monitoring personal communications on work devices in a misconduct situation

- Practical steps:
  - Consider other means of investigation
  - Check privacy notice
  - Document formal or informal DPIA
  - Do not review obviously private and irrelevant information
  - If relevant evidence may include private information, document justification for looking at it
  - Limit circulation of evidence obtained



Limits on monitoring work email access on personal devices in a misconduct situation

- Unless the employee is using the device for work purposes, unlikely to obtain access to personal devices voluntarily:
  - May be able to monitor access to remote work systems, likely lower risk, as less expectation of privacy – access for work purposes
- If the employee uses a personal device for work:
  - Check technology – depending on how it is set up dictates access
  - Ensure you have good BYOD policy
  - If you can access private information, proceed with caution

Contact us

Catherine Taylor
Partner
T +44 20 7067 3588
E catherine.taylor@cms-cmno.com

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Beirut, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Strasbourg, Stuttgart, Tel Aviv, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

---

cms.law