

CPNI Employee IT Monitoring Insider Threat

Strictly confidential

Key Contact

Virginia Allen

Partner

One Fleet Place
London
EC4M 7WS

D +44 20 7246 7659

virginia.allen@dentons.com

Dentons UK & Middle East LLP

Contents

Introduction	3
Europe	5
Executive summary	6
United Kingdom	13
Commentary on existing case law	13
Trends that can be identified	18
Existing case law	19
Summary of existing legislation	38
Future legislation which may have an impact on employee monitoring	42
France	52
Commentary on existing case law	52
Trends that can be identified	53
Existing case law	54
Summary of existing legislation	68
Future legislation which may have an impact on employee monitoring	70
Germany	71
Commentary on existing case law	71
Trends that can be identified	72
Existing case law	73
Summary of existing legislation	96
Future legislation which may have an impact on employee monitoring	100
Spain	101
Commentary on existing case law	101
Trends that can be identified	103
Existing case law	104
Summary of existing legislation	110

Future legislation which may have an impact on employee monitoring	114
Belgium	115
Commentary on existing case law	115
Trends that can be identified	117
Existing case law	118
Summary of existing legislation	142
Future legislation which may have an impact on employee monitoring	147
North America	148
Executive summary	149
US	151
Commentary on existing case law	151
Trends that can be identified	152
Existing case law	153
Summary of existing legislation	173
Future legislation which may have an impact on employee monitoring	175
Canada	176
Commentary on existing case law	176
Trends that can be identified	178
Existing case law	179
Summary of existing legislation	194
Future legislation which may have an impact on employee monitoring	196
Australia	197
Commentary on existing case law	198
Trends that can be identified	199
Existing case law	200
Summary of existing legislation	221
Future legislation which may have an impact on employee monitoring	231
UAE	233
Commentary on existing case law	233

Trends that can be identified	234
Existing case law	235
Summary of existing legislation	236
Future legislation which may have an impact on employee monitoring	238
Asia Pacific	239
Executive summary	240
India	241
Commentary on existing case law	241
Trends that can be identified	242
Existing case law	243
Summary of existing legislation	250
Future legislation which may have an impact on employee monitoring	252
Singapore	254
Commentary on existing case law	254
Trends that can be identified	255
Existing case law	256
Summary of existing legislation	257
Future legislation which may have an impact on employee monitoring	258
Latin America & Caribbean	259
Brazil	260
Commentary on existing case law	260
Trends that can be identified	261
Existing case law	262
Summary of existing legislation	270
Future legislation which may have an impact on employee monitoring	271
New and Emerging Technologies	272
United Kingdom Annex – detailed case reports	284

Introduction

Dentons UK and Middle East LLP are delighted to present this report in relation to the legal aspects of employee IT monitoring.

This project was commissioned by CPNI with the intention that the output report would serve as a legal resource for IT security personnel to better understand the legal risks faced when monitoring employees, specifically in the context of targeting insider-threat activity. The focus of the project was initially to be one looking at case law in a number of specified jurisdictions but the scope of this was extended to include a brief summary also of the legislation applicable to employee IT monitoring in each jurisdiction. **This report is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. It is not a comprehensive report of all the information or materials that are relevant to this area of law, and does not address any particular concerns, interests, value drivers or specific issues you may have. This report is current as of the date of publication and Dentons owes no duty to you to update the content of the report at any time for any reason. Please note this report does not represent the views of Dentons.**

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. Dentons is not responsible for any loss which may arise from any reliance on this document.

It was recognised at an early stage of the project that the case law review was unlikely to yield many cases specific to insider-threat activity. For this reason, the report seeks to analyse cases which are relevant more broadly to employee monitoring, since the legal principles which have emerged from those cases remain very relevant to employee IT surveillance, including in relation to insider-threat related monitoring. We have sought to identify any trends within this case law that can be seen from its development over time.

The scope of the review carried out by this report extends to the UK and eleven other jurisdictions namely France, Germany, Spain, Belgium, the US (certain states), Canada, Australia, the UAE, India, Singapore and Brazil. Given the length of the report, we have sought to include executive summaries where appropriate in relation to geographic regions. These high-level summaries however are not intended as a replacement for the fuller content, to which the reader must be directed, in order to understand the legal position in relation to any specific country.

This report seeks not just to consider the existing position in relation to employee IT monitoring but also to look at what the future might hold in store, both in terms of future legislation within this area as well as in relation to new and emerging technology. For that reason, we have sought, wherever possible to indicate the future direction of travel so far as legal restrictions on employee IT monitoring are concerned.

In the EU, a key development at the time of writing is the requirement to comply with the General Data Protection Regulation (**GDPR**) with effect from 25 May 2018. Given this new Regulation is likely to have a significant impact on employee IT monitoring within the EU, it is dealt with specifically within this report.

Note that any Europe-wide future legislation (such as GDPR) or any case law of the European Court of Human Rights, is dealt with within the UK chapter, so as to avoid repetition within the other European chapters for France, Germany, Spain, and Belgium and should also be taken into account for those countries accordingly.

The report also considers how the law might be applied or respond to new and emerging technology including big data, artificial intelligence and machine learning, biometric monitoring, wearables and dark web monitoring. It

is of course not possible to predict with any certainty what the future may have in store and the research to produce this report was undertaken during January and February 2018, so the law can be considered stated as at that time.

Dentons UK & Middle East LLP

March 2018

Europe

Executive summary

The following high-level thoughts can be offered having regard to the position on IT monitoring within Europe:

- It is clear in the context of this overall report that the most stringent restrictions on employee monitoring arise from legal jurisdictions in Europe;
- This does not come as a particular surprise given the convergence of data protection laws required by the EC Data Protection Directive 95/46;
- The Directive sets down clear requirements as to fairness and transparency for specified purposes, as well as the need for any data processing (such as employee IT monitoring) not to be excessive in relation to those purposes;
- A need for transparency and proportionality is emphasised in all of the individual country summaries within Europe dealt with in this report and can be seen as two clear fundamental requirements within the EU;
- This trend towards convergence is of course set to continue with the more onerous requirements of the General Data Protection Regulation (**GDPR**) which will implement even stronger and more uniform requirements, including as to transparency of data processing, across the European Union;
- The impact of GDPR (discussed in detail within the UK chapter) cannot be underestimated: not least given the influence it is likely to have beyond the confines of the EU. This can already be seen in the UK, which regardless of Brexit, is widely anticipated to be unlikely to depart in material respects from GDPR standards. This in part reflects the future importance of the UK being seen to provide adequate data protection standards to allow continued export of personal data from countries remaining in the EU;
- While this report has the context of IT security monitoring firmly in mind, it can be seen from the individual country reports that the case law summaries rarely involve insider threat activity, such as industrial espionage or intention by employees to defraud or exploit confidential information. The reasons for the lack of specific case law in the context of insider threat activity is further explored in the commentary on UK case law;
- What can be seen instead, is that the vast majority of reported cases, across the EU jurisdictions surveyed in this report, relate by way of subject-matter to situations of video surveillance, of social media misuse or, for example, excessive personal use of company IT systems by employees;
- These cases typically focus on how clear the employer's policy is, the business need for the monitoring, how proportionate the employer's response has been and the severity of the conduct in question;
- Some jurisdictions (such as France) also take a stricter approach to the issue of admitting evidence which has been improperly obtained by employers. For this reason, a significant number of cases also deal with this issue. This exclusion of evidence will often have fatal implications for employers defending employment claims in practice, if they are unable to rely on the evidence obtained which establishes, for example, gross misconduct having been committed;

- That said, in some jurisdictions such as Belgium, as will be seen, there has been a softening of approach in that respect. Employers should however be very cautious, particularly in continental Europe in relation to this issue; while in the UK a more lenient approach is generally taken to the question of admissibility of improperly obtained evidence, provided it can be established to be relevant to the proceedings;
- A further notable point which can be made in connection with Europe is that the European Court of Human Rights has shown an increased willingness to defend privacy rights in the context of the workplace. That such rights extend to the workplace has long been asserted but there are now a number of notable recent cases (discussed in the UK chapter) which considers how this operates in practice;
- For example, in *Barbulescu v. Romania* (2017), a Grand Chamber of the European Court of Human Rights considered the position where an employer has prohibited all personal use of work IT equipment and thereafter dismissed an employee for personal use in breach of that restriction;
- The Court was faced there with how to reconcile the right of personal privacy extending to the workplace, with a policy that sought to remove any such expectation, in the context of use of the employer's IT system. It took the view that an employer could not, by way of instructions (or policy), reduce private social life in the workplace to zero. Respect for private life and correspondence continued to exist, even if restricted so far as necessary;
- In any event, the Court held in that case there had been a failure to give prior notice to the employee of the nature and extent of the monitoring (including content of communication) that may take place. As such, the dismissal was held to have breached the employee's rights under Article 8 ECHR to private life. *Barbulescu* sends a very clear message to employers, in the specific context of IT monitoring as to the fundamental need for the two key requirements discussed above, of transparency and proportionality and that workplace privacy cannot be completely removed;
- This principle has since been further developed by the European Court of Human Rights in its recent case law;
- In *Antovic and Mirkovic v. Montenegro* (2017) two professors successfully established a breach of their right to private life in the workplace under Article 8 arising from their employer installing video surveillance in university lecture theatres. The Court said the lecture theatres were not just for teaching: it was a place for professors to interact with students, to develop social relations and thus constructing social identity at work. Continuous video surveillance amounted to a considerable intrusion and required evidence of the necessity of the measure, which could not be established in that case;
- While the following summary **should not be relied upon in place of the detail given in relation to each country**, the following high-level observations can be made in relation to the countries reviewed within the Europe section:
- In the **UK** broadly speaking, a slightly more permissive approach appears to be taken in the context of employee IT monitoring. The law on employee monitoring is found within statutory human rights, telecommunications and in particular data protection law, as well as within the body of case law;

- While the requirements of fairness, transparency and proportionality certainly apply as elsewhere in Europe, evidence which is obtained in breach of those requirements, will normally be deemed admissible, provided they are relevant to the proceedings and there is not a public policy reason to exclude the evidence;
 - Courts and tribunals thus far have also appeared to take a common sense approach to, for example, social media misuse by employees. Where an employer can evidence damage having occurred to its reputation, this typically has been found to justify the interference with any right to privacy asserted by the employee. An example can be seen in the case of *Game Retail v. Law* where the dismissal of an employee for sending offensive tweets on Twitter was upheld, it being found to have had the necessary impact on the employer;
 - Similarly where the conduct in question involves fraud or dishonesty, as in cases discussed in the chapter such as *McGowan v. Scottish Water* or *City and County of Swansea v. Gayle*, courts have typically taken a robust view of the employer's right to investigate (including in both those cases by way of covert video surveillance) and dismiss for such misconduct;
 - In comparison with the other European countries reviewed within this report, UK courts appear to be more receptive to employers who can demonstrate harm caused to them, which can be established by way of having carried out monitoring, including in relation to the admission of evidence;
 - That said, it is clear there are limits and where that harm cannot be established – for example, in cases such as *Smith v. Trafford Housing Trust* – which involved an employee expressing negative opinions on gay marriage on his personal Facebook page, the courts are more likely to uphold an argument based on personal privacy and the right to freedom of expression.
- This more lenient stance can be contrasted with the position in **France**, where a stricter approach appears to be taken, both in relation to rules in relation to individual personal privacy rights and the admissibility of evidence:
 - As well as the case law and data protection law, attention needs to be given to both the French civil code (regarding the right to privacy and secrecy of correspondence) and also the labour code;
 - Much of the case law reported is concerned with the issue of whether the employer can rely upon evidence obtained given the restrictions imposed on employers;
 - This includes case law on the misuse of social media such as *Jesana v. X* where an employer was found to have breached the privacy rights of an employee by accessing her personal Facebook page using the mobile telephone of a work colleague;
 - This strong protection for personal privacy rights, can also be seen in the case of *OPH v. Le G* where an employee posted death threats against work colleagues on Facebook which were passed to the employer. While in the UK this would be unlikely to present an issue for the employer using such material against the employee, in this case the Versailles Court of Appeal determined the employer could not base a dismissal on the Facebook material because the page was configured to be limited to the employee's friends, so it was not of a public nature;

- This has been extended beyond IT monitoring to aspects such as geolocation monitoring (*Eller Lubricants* case: use of geolocation data for performance dismissal held to be disproportionate);
 - It can be seen that a much stricter position therefore appears to be taken such that a failure to comply with French legal requirements as to employee monitoring, which are themselves detailed, is likely to mean the evidence obtained cannot be used against the employee;
 - Note that monitoring may also be required to be declared to the CNIL (the French Data Protection Commission).
- We also find more detailed requirements in **Germany**, including those which arise from general privacy rights within the constitution, from federal data protection law and applicable works agreements as well as case law.
 - The monitoring of employees is identified as triggering a co-determination right by the works council;
 - The summary of the case law provided indicates the key factors taken into account by the courts in Germany and that the admissibility of evidence can also be an issue where improperly obtained;
 - The importance of proportionality is clear with a trend identified of it being difficult for an employer to justify permanent monitoring, given the need to ensure that regardless of the reason for the measure (i.e. such as the risk of high financial loss), the employer has to be able to identify that their actions resulted in the "*least restrictive*" means to achieve that objective. Covert monitoring is identified as particularly difficult to carry out;
 - Some interesting examples can also be found within the case law in Germany, which are specific to IT monitoring;
 - In the case 2 AZR 681/16 the Federal Labour Court looked at an employer's use of an IT tool "KeyLogger" which enabled each keyboard input of employees to be monitored, in circumstances personal use was not permitted. In that case, an employee was dismissed for having downloaded a computer game and having used email in relation to a personal family business interest. The employer argued privacy rights did not apply on the basis that it had communicated a ban on personal use of work equipment to all employees;
 - The Court held that while misconduct had taken place, it was not sufficiently serious to justify dismissal in this case. Moreover, it held that the KeyLogger tool involved the processing of personal data and a breach of the employee's privacy rights. While it could be legally permissible for an employer to monitor openly on a random basis to check compliance with policies, this did not extend so as to permit continuous monitoring without sufficient reason;
 - The Court also separately upheld the exclusion of this evidence in breach of privacy rights;
 - Cases in relation to the misuse of social media are also reported from Germany: in one case an employee was found fairly dismissed for calling his superior an "oppressor", an "exploiter" and a "stupid shit" on Facebook; whereas in another, a dismissal for insulting a superior "by the use of

"emoticons" which involved emoticons showing a pig's head and a bear's head to represent supervisors, was found to be too harsh.

- In **Spain**, we find restrictions arising from case law, data protection and employment legislation, collective bargaining agreements and from the Spanish constitution, as detailed in the summary of legislation.
 - The case law in relation to IT monitoring can be summarised by saying that "*monitoring measures must be suitable, proportional and necessary and the employee must be aware of them*". Individual assessment is identified as being required on a case to case basis as to whether proportionality is satisfied;
 - It appears that the key requirements applicable to IT monitoring include there being a specific, explicit and legitimate purpose, the monitoring being a proportionate response to the threat, there being minimal repercussion to the intimacy right of employees and also, notably, that the employee or their representative must be present when an employee's email is accessed;
 - Where these requirements are not met, there is a high risk of evidence being declared null and void by a Court;
 - That said, the discussion as to trends within case law identifies that there is at present some legal uncertainty over the status of IT monitoring. This arises from a reported disconnect between Spanish domestic case law (which appears to give greater freedom to corporate control) and the case law of the European Court of Human Rights (such as the *Lopez Ribalda* case) which takes a stricter approach in the context of employer video surveillance;
 - It is anticipated in this respect that the domestic case law will be modified to be brought into accordance with the European Courts of Human Rights (**ECtHR**) ruling and it therefore being advisable to proceed in accordance with that ruling. Note this case of *Lopez Ribalda* is more fully summarised within the UK chapter (which deals with all the relevant ECtHR case law);
 - A further example of IT monitoring can be seen in the case of *Quorum Gestión Empresarial* which involved the improper monitoring of an employee's email including correspondence sent to his lawyer, including in relation to litigation strategy in a case concerning the employer. The case appears to draw upon the ECtHR case of *Barbulescu* and considers what is required by an employer having regard to Spanish law.
- Finally, in relation to **Belgium**, the legal framework in relation to employee monitoring includes consideration of the right to privacy within article 22 of the Belgian constitution as well as separate privacy, employment and telecommunications legislation and collective bargaining agreements (including one which specifically clarifies the conditions under which employee communications may be monitored).
 - The review of case law indicates (as set out within the commentary) that it must be read alongside the Belgian legal doctrine regarding illegally obtained evidence. This notes the traditional view being that such evidence must be excluded and not taken into account;
 - Since then there appears to have been a departure from the strictness of this position with the case of *Antigoon* in 2003 setting down the three situations where a Court must rule out such

evidence: (a) where the consequence of nullity is prescribed by law; (b) where the illegality in obtaining the evidence has tainted the reliability of it; or (c) where relying on the evidence would be in violation of the right to a fair trial;

- Developed further since then, further factors a Court may take into account include whether the illegality was intentional, whether the degree of seriousness of the illegality is disproportionate to the value of evidence and whether it proves the material elements of a crime and not the intent of the perpetrator;
- This case law has since been applied in employment cases – as can be seen from the case of *Manon* which involved evidence of an employee who worked in a chocolate store stealing from a cash register, obtained by a camera installed in violation of the legal framework. The case confirms that it is for the court determining the case to decide whether or not the *Antigoon* principles have been satisfied;
- Since then, as the chapter notes, there has been an identifiable trend by way of a growing tendency to accept evidence in employment-related cases which have been gathered in violation of the applicable legal standards but that some absolute limits remain;
- This can be seen, for example, in the case from the Labour Court of Antwerp dated 2 September 2008 where an employer conducted a random check of personal use of the internet and email. Although the employee argued this violated the right of secrecy for telecommunications, the Court ruled the illegality was of a minor character and therefore could be used in evidence;
- The other trend identified in employment related case law is that it is more and more accepted that private statements on social media may have an impact on the employment relationship and may lead to an employee's termination;
- Like other jurisdictions, the case law here indicates that the seriousness of the issue is likely to be highly determinative of whether a dismissal for gross misconduct might be upheld by the courts, although there are signs of a fairly lenient approach taken towards employees in some of those cases;
- For example, the case reports give an example where an employee (who was also a trade union rep) made negative statements regarding his employer, as well as his direct manager on Facebook on the page of the supermarket he worked for (with the content apparently visible only to his co-workers at the same level). While the court agreed that the employee had erred, violating his duty of loyalty, it did not consider the facts to amount to gross misconduct, so as to justify immediate termination of his employment relationship;
- Other instances of the courts in Belgium taking such a lenient approach to social media misconduct can also be seen. Another example given in the case reports relates to an employee who made racist comments regarding a work colleague on her Facebook page. The tribunal decided that having regard to the context of the statements an official warning would have been warranted but not an immediate termination for gross misconduct;
- This can be contrasted with other instances where a more serious view has been taken of such conduct. This includes the Labour Court of Brussels appeal judgment of 3 September 2013

involving an employee dismissed for making negative statements about his employer on his own Facebook page, which also falsely presented his job role at work;

- Upholding his termination of employment, a distinction was drawn between the personal and public use of Facebook with the court saying different reasonable expectations of privacy depending on the area in which comments were posted or made and whether or not they were publicly accessible;
- Similarly in its judgment of 12 September 2014, the Labour Court of Brussels appears to have gone further and held that even if comments on a Facebook page was only visible to a user's personal network, an employee may still not be able to hide behind the right of privacy where the employer can show a level of publicity leading to substantial damage.

United Kingdom

Commentary on existing case law

The rise in insider threat activity

The review of case law in relation to employee monitoring may, if not placed in the proper context, risk giving a misleading impression as to the incidence and risk of insider threat activity.

The threat to UK businesses from insider threat activity has arguably never been greater. One need only refer to the case of *Various Claimants v. WM Morrison* to see the damage that can be wrought by one rogue employee. There a disgruntled IT auditor, trusted by his employer with highly confidential personal data in relation to 100,000 employees, who had previously tried to access the Dark Web at work, uploaded the personal data onto a file sharing website and sent it to three newspapers. Their personal information (including names, addresses, national insurance numbers and bank details) having gone public, employees of the supermarket obtained damages against Morrisons in the High Court, on the basis they were found to be vicariously liable for the wrongful actions of their rogue employee.

That legal challenge, as will be seen from the case law review, remains for the moment somewhat unique. But although the class action brought by affected work colleagues might be seen as the first of its kind, it is highly unlikely to be the last. Employers face the risk of insider threat activity on a daily basis.

There remains however a disconnect with the number of reported employment law cases which deal specifically with insider threat monitoring, where rogue insiders have been dismissed by their employers and have challenged their dismissal leading to an examination by the courts of the monitoring techniques deployed.

A number of factors most likely explain this discrepancy between incidence and risk of insider threat activity and reported case law.

The most obvious factor however is that an employee who has been caught red-handed involved in serious issues of fraud, or the disclosure of sensitive or confidential information, is highly unlikely to wish to incur the legal costs of bringing an unfair dismissal claim they are unlikely to succeed in. The Morrisons example above is a case in point. The rogue employee in that case was convicted and sent to prison for offences under the Computer Misuse Act 1990 and the Data Protection Act 1998. But for the novel challenge brought by the impacted employees, the facts and circumstances would never have entered into case law.

A related factor is that rarely will a first instance decision (i.e. lower court decision such as an Employment Tribunal judgment or High Court decision) be widely reported, unless there is some novelty or an interesting point of law involved. The bulk of the case law review therefore comes from reported appeal level cases. This in itself requires there to be a debatable point of law at issue, before an appeal court will accept the case. In turn, this leads to the canon of case law on employee monitoring being necessarily selective in nature. It is perfectly possible that rogue insider threats have perhaps challenged their dismissals before Employment Tribunals, but their decisions not deemed worthy of reporting.

An employee is far more likely to challenge his or her dismissal and invite scrutiny of the employer's methods of monitoring and decision to dismiss, in circumstances where there is at least a reasonable prospect of success. This in turn lends itself to situations either where the internal misconduct in question, might be argued (at least by the employee) as being of a less serious nature or where the monitoring is seen by the employee as having

been wholly disproportionate (or possibly a combination of both). This is borne out in practice when one reviews the cases within the case law review.

Indeed, a clear example of this can be seen in the number of cases which have now been reported relating to dismissals of employees arising from their employer's monitoring of their social media activity, where often the level of impact of this conduct on the employer has been debatable. In such a scenario, a challenge is far more likely to be brought and such cases, with a degree of novelty involved, have an increased prospect of reaching an appeal court and becoming reported within case law.

The limits of monitoring being set by non-insider threat cases

What this means of course is that the body of case law which provides us with guidance on the limits of employee monitoring, including in the context of insider threat activity, is being developed by cases not generally involving insider malicious activity (so far as leaking confidential business information is concerned).

It is vital to recognise however that the approach being taken and principles applied by courts and tribunals relating to employee monitoring in the context of these different subject matters (whether social media misuse or the use of covert video surveillance) would be the same principles of law set down by the appeal courts that would be brought to bear if and when insider threat cases arise.

So while the privacy versus monitoring debate is often taking place in a slightly different context, the relevance of where the line is being drawn remains highly relevant to insider threat activity and clear lessons and trends emerge from that case law.

A relevant question might be whether there is a potential downside to these principles or lessons being developed in this wider context of employee monitoring. For example, might it be of concern to companies focussed on combatting insider threat activity, that courts and tribunals are developing these principles in situations where the risk to the organisation is less severe? For example, the dissemination of highly sensitive business information is not comparable with the reputational damage that might or might not arise from a embarrassing social media post. Is there a wider risk that any principles emerging from case law might set the thresholds for fair employee monitoring too highly arising from the cases that make it to a tribunal or court?

The case law would suggest this not to be the position and that, perhaps unsurprisingly, courts and tribunal are adept at placing greater emphasis on the business need for monitoring where very serious wrongdoing, such as fraud, is at stake. The case of *McGowan v. Scottish Water* provides an example where extensive covert video surveillance of an employee's home (albeit in the unusual situation of employer provided tied accommodation) was held proportionate to Scottish Water establishing his fraudulent activity and their responsibility as a public authority to duly protect their assets.

One can also see this in cases such as *Turner v. East Midland Trains Ltd* (a ticket inspector fraudulently selling faulty tickets) or *City and County of Swansea v. Gayle* (a local authority employee playing squash at a sports club while clocked in at work) where in both cases the right to privacy under Article 8 of ECHR could not be used to bring fraudulent conduct within a reasonable expectation of privacy.

These cases can be contrasted with those where the issue at stake appears to be less serious and the monitoring and response appears disproportionate: such as a photo of a rugby player's bare bottom being uploaded to Twitter – where the employer's dismissal was seen as a clear overreaction: *Mason v. Huddersfield Giants Ltd.*

What key principles emerge from this body of case law?

A number of key principles emerge from the case law review which are relevant to monitoring insider threat activity.

The first of these and the starting point is the recognition by the courts that the right to privacy under Article 8 ECHR can and does extend to the workplace. This has been long recognised by the European Court of Human Rights and a number of cases that have looked in particular at monitoring employee communications.

Copland v. United Kingdom illustrates that monitoring employees without a clear policy advising that monitoring may take place is likely to give rise to a breach of Article 8.

However, of perhaps more interest to those who draft and implement IT and security policies is *Barbulescu v. Romania* which found a reasonable expectation of privacy applied to personal instant messages sent using work equipment even where the employer had a policy which prohibited any personal use by employees. The message from this case is clear: while IT policies can set parameters and may well be relevant to the level of privacy expectation employees have, a policy cannot by itself remove all expectations of some level of privacy at work. This extends nowadays to electronic communications as much as it does to the locker room.

The second principle which clearly emerges is the need for monitoring to be proportionate to the risk. If the same result can be achieved in a less intrusive way, the monitoring may be considered disproportionate and unlawful. This has been recognised within both domestic case law (in *McGowan v. Scottish Water* the EAT accepted Scottish Water has satisfied itself it was not possible to investigate the fraud using less intrusive means) but this has been particularly developed by the European Court of Human Rights (**ECtHR**) in very recent case law.

Two recent Strasbourg cases give clear examples of the need for proportionality. In the case of *Lopez Ribalda v. Spain* (January 2018) the employer (a Spanish supermarket) installed covert video cameras facing checkout counters to detect theft and the ECtHR held this to be disproportionate and in breach of Article 8. This was because the employer could have advised the employees of the video surveillance taking place and had not done so.

A case decided by the ECtHR just before *Lopez Ribalda* and which goes even further is *Antovic and Mirkovic v. Montenegro* (November 2017). In that case, the use of visible surveillance cameras in a university lecture theatre was successfully challenged by two professors as breaching their right to a reasonable expectation of privacy at work under Article 8, where there was no evidence of risk to students as had been claimed. What can be seen in this case in particular is the ECtHR pushing back strongly against an ever-increasing surveillance society and using the right to a reasonable expectation of privacy in the workplace as a weapon to do so.

Both cases point to the fact that an employer cannot simply point to a risk and deploy whatever monitoring it considers appropriate to address that risk. The developing Article 8 case law points for there to be a need for a considered assessment of the risk and for any interference with privacy to be proportionate. In this respect, the Article 8 case law appears to be aligning itself with that which is required separately under data protection legislation, which is discussed separately within this chapter.

The third principle is the vital importance of a clear policy setting out the parameters of monitoring which may take place. The case of *Copland v. United Kingdom* has already been mentioned, where a UK further education college failed to advise an employee that her communications may be subject to monitoring. This has also often been an important factor in the cases involving social media misconduct – whether employees were advised this might take place and when they might be disciplined for breaching social media policies.

Again, this is an area where the legislation will shortly require much more and as discussed below in the context of GDPR requirements, it is likely that employers will have to specify not just a bland statement that monitoring may take place, but provide details of how that monitoring will be carried out in practice.

The fourth principle has already been discussed above: that courts and tribunals will have regard to the severity of the misconduct or business risk faced. Cases involving fraud, deception, or disclosure of sensitive confidential information are not treated in the same way as the reputational damage that might arise from the expression of controversial views such as gay marriage on Facebook: *Smith v. Trafford Housing Trust*.

That said, it can be seen from cases such as *Lopez Ribalda* that it is not enough just to point to a very serious risk (in that case suspected theft) where the monitoring itself to address the risk was deemed disproportionate.

The final key principle relates to the admissibility of evidence. A number of cases within the case law review involve the court or tribunal having to consider whether it is prepared to admit and hear covertly obtained evidence. A number of these cases have arisen in fact from objections taken by employers to secret recording made by employees at their workplace.

These cases are all relevant to insider threat activity since if improperly obtained evidence will not be accepted by a court or tribunal (due to alleged interference with Article 8 rights, for example) it substantially increases the risk for employers associated with monitoring which may be deemed excessive and disproportionate.

As will be seen from the case law review, by and large courts and tribunals have been prepared to accept improperly obtained or covertly recorded evidence provided that the evidence is relevant to the issue before the court: *Vaughan v. Lewisham LBC*. However, it can also be seen that a limit on admissibility can arise from public policy considerations with *Amwell View School v. Dogherty* giving an example where the secret recording by an employee of an appeal hearing was found admissible but not the private deliberations of the panel.

This illustrates that whether for employers and employees, the admissibility of covertly obtained evidence, even where relevant, is subject to limitations. It also seems likely the more egregious invasion of personal privacy, perhaps the less likely a court will look sympathetically on an admissibility issue.

The implications for IT security monitoring aimed at insider threat?

As discussed above, these key principles emerging from case law, are likely to be applied by courts and tribunals in the same way in relation to IT security monitoring aimed at insider threat. There is no particular reason to treat such cases any differently, although the severity of the risk will no doubt be a relevant consideration, particularly where monitoring is being deployed to protect critical national infrastructure.

It should not present too significant an issue to ensure that robust policies are in place to support IT security monitoring. The issue of proportionality should not be too difficult to correctly balance where critical risks are being guarded against. The case law points generally to the need for monitoring to be specific, targeted and transparent and in this respect it has started to converge with the requirements of data protection law.

It is also important to recognise that the case law presently says nothing in relation to the additional and stricter requirements which arise, for example, in relation to GDPR when introduced on 25 May 2018. While a convergence is taking place in relation to how personal privacy at work is viewed, the most significant limitations to employer monitoring arise not from these principles emerging within case law but from the more detailed and specific requirements of this legislation, as discussed in detail below.

By its nature case law will always lag behind both new legislative developments but also new and emerging technological developments. This can be seen in the time it took for case law to be reported in relation to social media misuse, with only the first ever Employment Appeal Tribunal decision in relation to the misuse of Twitter taking place in November 2014, many years after the rise in popularity of the platform.

It cannot therefore be expected that existing case law has much to say about artificial intelligence or wearables or user-entity behavioural analytics, beyond the likely application of key principles in relation to privacy and the workplace.

The more prominent and important role in this respect is being carried out not by the courts, but for example by the Information Commissioner's Office (**ICO**) or the Article 29 Working Party and its detailed guidance on how GDPR might be applied in the context of monitoring at work and new technologies. An understanding of the case law is certainly important but it can perhaps be best seen as providing the backdrop to the specific detail that privacy laws such as GDPR will require in future.

Trends that can be identified

A number of trends can be identified from the case law which has emerged to date. These include the following:

- The notion of a reasonable expectation of privacy within the workplace (which cannot be removed simply by policy) is being further developed by the courts
- There is a growing confidence on the part of the ECtHR to stand up for and assert privacy rights under Article 8 in the workplace – as can be seen from the two recent decisions finding workplace surveillance to have been unlawful
- The need for proportionality in particular has emerged as a significant level which courts can deploy in relation to excessive monitoring
- Employees appear more ready to raise privacy arguments in relation to monitoring – whether in relation to their use of electronic communications or their social media use – pointing to increasing expectations of personal privacy
- The social media dismissal cases that have arisen have also shown that courts and tribunals will draw a line between social media use which has clear impact on the employer and that which does not. Employers need to be careful not to take a kneejerk reaction towards social media misconduct
- Although not raised in the cases to date, the abolition of employment tribunal fees by the UK Government has already led to a significant increase in the number of claims brought, a trend that seems likely to continue.

Existing case law

List of cases

1. *Avocet Hardware v. Morrison* EAT/417/02 (page 19)
2. *McGowan v. Scottish Water* EAT/0007/04 (page 20)
3. *Amwell View School Governors v. Dogherty* EAT/0243/06/DA (page 21)
4. *Copland v. United Kingdom* (2007) 45 EHRR 37 (page 22)
5. *Fosh v. Cardiff University* EAT/412/07 (page 23)
6. *Turner v. East Midlands Trains Ltd* [2012] EWCA Civ 1470 CA (page 24)
7. *Smith v. Trafford Housing Trust* [2013] IRLR 86 (page 25)
8. FCA Final Notice in relation to Christopher Niehus (page 26)
9. *City and County of Swansea v. Gayle* [2013] IRLR 768 (EAT) (page 27)
10. *Vaughan v. Lewisham LBC* UKEAT/0534/12 (page 28)
11. *Mason v. Huddersfield Giants Ltd* [2013] EWHC 2869 (QB) (page 29)
12. *Game Retail v. Laws* EAT/188/14 (page 30)
13. *British Waterways Board (t/a Scottish Canals) v. Smith* UKEAT/4/15 (page 31)
14. *Garamukanwa v. Solent NHS Trust* (EAT/245/15) (page 32)
15. *Barbulescu v. Romania* [2017] IRLR 1032 (page 33)
16. *Antovic and Mirkovic v. Montenegro* [2017] ECHR 1068 (page 34)
17. *Various Claimants v. WM Morrison Supermarket Plc* [2017] EWHC 3113 (QB) (page 35)
18. *Lopez Ribalda and Others v. Spain* Applications 1874/13 and 8567/13 (ECtHR, 9 January 2018) (page 36)

In addition to the case law summaries below, fuller case reports can be found in the United Kingdom Annex at the end of this document.

Case Name, Citation and Court	<i>Avocet Hardware v. Morrison EAT/417/02</i> Employment Appeal Tribunal
Date	23 September 2004
Subject	Monitoring of an employee's phone calls; employee's right to privacy and employer's right to a fair trial
Key facts	<ul style="list-style-type: none"> • M was employed by AH as a telesales operative. Without M's knowledge, AH monitored his calls. • When AH took exception to one of M's calls with a customer, M was dismissed summarily for gross misconduct. • M lodged an unfair dismissal claim with the Tribunal. In defending this claim, AH sought to use the recording of that particular phone call, but the Tribunal refused. • A appealed against this decision to the Employment Appeal Tribunal (EAT).
Key points	<ul style="list-style-type: none"> • The EAT accepted AH's evidence might have been obtained in breach of Article 8 but held that AH's right to a fair trial under Article 6 had to be considered since the contents of the telephone call were crucial to their justification for dismissal. • It held that the telephone recording had to be allowed in evidence regardless of the method by which it was obtained.

Case Name, Citation and Court	<i>McGowan v. Scottish Water EAT/0007/04</i> Employment Appeal Tribunal
Date	23 September 2004
Subject	Video surveillance of an employee outside work; right to privacy
Key facts	<ul style="list-style-type: none"> • M was employed at S's water treatment plant and lived nearby. • S became suspicious that self-completed timesheets in respect to call out time were being falsified. As such, S considered the possibility of putting cameras inside the process plant, but this was deemed impractical. • Consequently, S employed private investigators who hid themselves opposite M's house and filmed him coming and going. M was subsequently dismissed. • After the initial Tribunal, the issue of whether Article 8 was breached by the covert surveillance of M's home, and if this breach would have made the dismissal process unfair was referred to the Employment Appeal Tribunal (EAT).
Key points	<ul style="list-style-type: none"> • The EAT said that initially, covert surveillance of a individual's home raised a presumption that the right to have one's private life respected was being invaded. • In this case, however, the question of proportionality needed to be considered as the purpose of the surveillance was to witness how many times M left the house to go to the plant which would determine the accuracy of M's timesheets. Therefore, S's investigation went to the essence of the obligations and rights of a public corporation to protect its assets. As such it was not disproportionate. • The EAT dismissed the appeal.

Case Name, Citation and Court	Amwell View School Governors v. Doherty EAT/0243/06/DA Employment Appeal Tribunal
Date	16 June 2006
Subject	Admissibility of secretly recorded evidence
Key facts	<ul style="list-style-type: none"> D was subject to disciplinary proceedings which consisted of three "<i>public hearings</i>" followed by "<i>private deliberations</i>" which resulted in her subsequent dismissal. At the Tribunal, it was discovered that D had recorded the "<i>public hearings</i>" without the knowledge of the panel members.
Key points	<p>The Employment Appeal Tribunal (EAT) held:</p> <ul style="list-style-type: none"> The Tribunal had not erred in law in admitting evidence which had been disclosed late, finding that the Tribunal's order that the original hearing be adjourned and that D should pay the costs already incurred was reasonable. As the governors worked in the public domain, their private lives could not be violated and Article 8(1) was not engaged. The recordings had been made clandestinely, but not illegally. The governors were simply acting in the same capacity as a panel of senior managers of any other employer and exercised no obvious judicial function. D could not use parts from the private deliberations in her evidence. It concluded that there was an important public interest that parties should comply with the "<i>ground rules</i>" on which disciplinary and appeal proceedings.

Case Name, Citation and Court	Copland v. United Kingdom (2007) 45 EHRR 37 European Court of Human Rights
Date	3 April 2007
Subject	Employer monitoring of employee data; right to privacy
Key facts	<ul style="list-style-type: none"> C was employed as an administrator at a college. At the deputy principal's orders, C's telephone, internet and email use were monitored in order to check if she was using them excessively for her own personal use. C contended that her personal movements, both at work and when on leave, were the subject of surveillance and that legally privileged materials were seen by the deputy principal. The parties disputed the extent and duration of the monitoring and the case was referred to the European Court of Human Rights as set out below.
Key points	<ul style="list-style-type: none"> The Court confirmed that telephone calls from business premises were covered by the terms "<i>private life</i>" and "<i>correspondence</i>" for the purposes of Article 8(1). Therefore, emails sent from work and information derived from the monitoring of personal internet usage would also be protected. On the basis that C did not know that her work calls, emails or internet usage were being monitored, the court stated that it was reasonable for her to expect that her privacy would be respected. Even if the monitoring was not as extensive and intrusive as C claimed, the collection and storage of C's personal information which the government admitted had taken place without her knowledge would itself amount to an interference with C's Article 8 rights. Court held that Article 8 had been violated because: <ol style="list-style-type: none"> 1. The government's statutory powers did not give it an absolute right to do anything necessary and expedient for the purposes of providing further and higher education. 2. There was no domestic law regulating monitoring of communications at the relevant time; and 3. The college had no policy informing employees that they could expect such monitoring to take place.

Case Name, Citation and Court	Fosh v. Cardiff University EAT/412/07 Employment Appeal Tribunal
Date	23 January 2008
Subject	Search of employee's email account; right to privacy
Key facts	<ul style="list-style-type: none"> F was a professor working for the respondent university, C. Despite the fact that C told him to stop on grounds of conflict, F supported a student in bringing a claim of race discrimination against C. F was also accused by C of disclosing confidential information to the student. F was dismissed following a disciplinary investigation that involved a search of F's email account. The findings included inappropriate communication with students via email and inappropriate involvement with the student who had made a race discrimination claim against C. F claimed unfair dismissal, victimisation (under the Race Relations Act) and automatically unfair dismissal for whistleblowing. The Tribunal found F's dismissal to be fair and that there was no victimisation. F appealed to the Employment Appeal Tribunal (EAT) alleging the dismissal was unfair in that the email was in breach of Article 8.
Key points	<ul style="list-style-type: none"> The EAT dismissed the appeal holding that the Tribunal made a clear finding that C had taken action as there was a perceived conflict of interest and breach of confidentiality. The EAT decided that C would not have breached Article 8 if it was an "<i>emanation of the state</i>". F's emails were searched in accordance with the university's internal rules and C could rely on the Regulation of Investigatory Powers Act 2000.

Case Name, Citation and Court	Turner v. East Midlands Trains Ltd [2012] EWCA Civ 1470 CA Court of Appeal
Date	16 November 2012
Subject	Fair procedure and Article 8 ECHR
Key facts	<ul style="list-style-type: none"> • T was employed as a senior train conductor by E. • She was dismissed for fraudulently selling faulty tickets and dishonestly keeping the proceeds.
Key points	<ul style="list-style-type: none"> • At the Court of Appeal, T argued that the consequences of her dismissal engaged her Article 8 rights under the ECHR as it resulted in: <ul style="list-style-type: none"> 1. Damage to her reputation caused by a finding of dishonesty; 2. The potential restriction on her ability to obtain other employment as a result of that finding; and 3. The damage to the social relationships with work colleagues. • T argued that the Tribunal should have adopted a “proportionality” test under Article 8(2) rather than applying the traditional “band of reasonable responses” test for unfair dismissal. • The Court noted that each of the alleged consequences set out above could in principle engage Article 8. • The Court confirmed the case law principle that Article 8 does not apply where an individual brings the consequences complained of on themselves. However, it also noted that case law confirms that an individual must have been shown to have committed any wrongdoing before that principle can be invoked. It also requires that the process leading to the determination of wrongdoing to be conducted properly. • It held that it cannot be proportionate to dismiss an employee with consequences that engage Article 8 in circumstances where the employer has reached that decision in a procedurally unfair manner.

Case Name, Citation and Court	<i>Smith v. Trafford Housing Trust [2013] IRLR 86</i> High Court
Date	16 November 2012
Subject	Employee's use of social media and communication with colleagues; reputation damage; Article 9 and 10 rights
Key facts	<ul style="list-style-type: none"> • S, an employee of T, posted anti-gay marriage comments on his personal Facebook page and exchanged comments on the page with colleagues from work. The page identified him as an employee of T. • Following complaints, T brought disciplinary proceedings against S, resulting in a finding of gross misconduct and a subsequent reduction in pay and a demotion. T took the view the posts amounted to a breach of T's Code of Conduct (promotion of religious views), a breach of the Equal Opportunities Policy (to treat colleagues with dignity and respect) and also brought T into disrepute. • S brought a claim for breach of contract in the High Court and also alleged breaches of Article 9 (freedom of religion) and Article 10 (freedom of expression).
Key points	<ul style="list-style-type: none"> • The High Court found in favour of S. • It was held the posts did not bring T into disrepute as it could not be concluded that they were made on T's behalf. S used Facebook for purely social purposes. • In relation to Articles 9 and 10, an employer could prohibit promotion of religious beliefs whilst at work, but it would be very unusual for an employer to impose on an employee in their personal life by a Code of Conduct incorporated into their employment contract. As the Facebook page wasn't work related, the Code of Conduct did not extend to it. • The Equal Opportunities Policy could not extend to all situations outside work where an employee came into contact with another employee, and if it did this could be a restriction on freedom of expression. Moreover, S's colleagues had voluntarily agreed to be his Facebook friends and engage with his views online.

Case Name, Citation and Court	FCA Final Notice in relation to Christopher Niehus
Date	18 November 2012
Subject	WhatsApp communications involving confidential client information
Key facts	<ul style="list-style-type: none"> N was an employee for Jeffries (Bank) and in his role had access to confidential information regarding client deals. On numerous occasions N used WhatsApp to share client confidential information to friends and another Jeffries' client. The messages were ultimately discovered by Jeffries when N voluntarily handed over his phone as part of an investigation into an unrelated complaint against him. He was suspended pending a disciplinary investigation.
Key points	<ul style="list-style-type: none"> The Financial Conduct Authority (FCA) found that he had communicated confidential information during a social gathering and that he had failed to act with due skill and care. As N freely handed over his phone to Jeffries for inspection, the legal issues over the extent to which an employer can monitor an employee's messaging on their mobile phone never arose in this instance. However, this situation raises the issue of employers' considerations when monitoring employees' use of instant messaging in the workplace. The main issues which will be scrutinised in these situations will be whether or not the employee had a reasonable expectation of privacy in relation to the communication. Monitoring is more likely to infringe an employee's privacy if the employer does not have an IT policy in place and the employee has not been informed that their use of IT systems might be monitored.

Case Name, Citation and Court	<i>City and County of Swansea v. Gayle [2013] IRLR 768 (EAT)</i> Employment Appeal Tribunal
Date	16 April 2013
Subject	Video surveillance of an employee during work hours; right to privacy
Key facts	<ul style="list-style-type: none"> S had been informed that their employee, G, had been seen playing squash at a sports club during work hours. S subsequently hired a private investigator who filmed G outside the sports club during work hours. G was dismissed but a Tribunal found the dismissal unfair. They held that G's right to a private life under the ECHR was violated and that the G had ignored its obligations under Data Protection Act 1998 (DPA). The Tribunal held that the investigation was far more comprehensive than necessary and therefore unreasonable. They also said a person defrauding an employer still has an expectation of privacy when carrying out those acts. S appealed to the Employment Appeal Tribunal (EAT).
Key points	<ul style="list-style-type: none"> The EAT overturned the decision holding that there was no expectation of privacy in the circumstances. Article 8 was not breached as the video was taken in a public place, G was at the sports club when he should have been at work and S was entitled to know where he was at the time. Further, it was held that by committing fraud G could have no reasonable expectation that his actions were private.

Case Name, Citation and Court	Vaughan v. Lewisham LBC UKEAT/0534/12 Employment Appeal Tribunal
Date	6 June 2013
Subject	Covert recordings at work; admissibility of evidence
Key facts	<ul style="list-style-type: none"> • V. suffered from depression and complained of discrimination whilst working for L. She gave accounts of communications with employees which she said could be verified by recordings she had made covertly. • V. brought a discrimination claim against L and applied to an Employment Tribunal to adduce the recordings in evidence, without actually providing any tapes. • The application was refused as V. could not satisfy the Tribunal as to the relevance as the recordings. Admitting the evidence was seen as disproportionate given the length of the recordings (over 40 hours) and cost of reviewing them. V. appealed to the Employment Appeal Tribunal (EAT).
Key points	<ul style="list-style-type: none"> • The EAT upheld the decision of the Tribunal but for different reasons. The EAT held that the Tribunal clearly had no means to form a view on the admissibility of the tapes. However, it could not be said that any of the recordings would not be admissible in evidence. • It could have been the case that parts of the recordings were relevant and should therefore been admitted. Thus if V. made a fresh application to a Tribunal with tapes and clear reasons as to their relevance, there may have been a different result.

Case Name, Citation and Court	Mason v. Huddersfield Giants Ltd [2013] EWHC 2869 (QB) High Court
Date	15 July 2013
Subject	Employee's use of social media; reputational damage of employer
Key facts	<ul style="list-style-type: none"> • M was a rugby player employed by H. During H's end of season night out M had a picture taken of his bottom by a team mate using M's phone. M's girlfriend uploaded the picture the next day and M deleted the tweet two days later. • M was dismissed for gross misconduct, H citing that he had brought the club into disrepute. H also stated the need for players to use social media responsibly. • M brought a claim in the High court for breach of contract, stating that his behaviour could not be regarded as gross misconduct. M also stated that the twitter account was purely personal and not work-related.
Key points	<ul style="list-style-type: none"> • The High Court held that M had been wrongfully dismissed. • It held that M had not acted deliberately and at most had not removed the post quick enough. It was also relevant that the conduct had taken place outside of work location and hours. • Putting the tweets into context, the High Court said that there was no obvious link between the twitter page and H and that there was nothing on the page describing M as an employee of H. • The twitter page was used predominantly for personal rather than work-related purposes and as such there could be little reputational loss by H.

Case Name, Citation and Court	Game Retail v. Laws EAT/188/14 Employment Appeal Tribunal
Date	3 November 2014
Subject	Employee's use of social media; reputational damage of employer
Key facts	<ul style="list-style-type: none"> • L had a private twitter account that did not identify him as an employee of G. However, he followed the twitter accounts of G's stores for which he had responsibility and 75 of the stores followed him back. • After G was notified of tweets posted by L an investigation took place and identified 28 offensive tweets. L was suspended for gross misconduct, G taking the view that the tweets were in the public domain. • L brought an unfair dismissal claim and was initially successful. The Tribunal found that Twitter was unrelated to his work and there was evidence of only a single colleague being affected. G appealed to the Employment Appeal Tribunal (EAT).
Key points	<ul style="list-style-type: none"> • The EAT allowed the appeal, holding that L's twitter followers were not merely social acquaintances. It was also relevant that L had not made use of available privacy restrictions and did not operate both a social and a work twitter account as he could have done. 65 of G's stores were following L and could have seen the offensive tweets. • The EAT said a balance had to be struck between an employer's reputational risk and an employee's right to freedom of expression. Generally, employees should have the right to express themselves, provided it does not infringe on their employment. In this case, a member of staff had felt strongly enough to complain about the tweets. • The EAT said that in cases of this kind factors that may be relevant include whether an employer has a social media policy, the nature of the misuse and whether any damage was done to customer relationships.

Case Name, Citation and Court	British Waterways Board (t/a Scottish Canals) v. Smith UKEAT/4/15 Employment Appeal Tribunal
Date	3 August 2015
Subject	Employee's work related posts on social media; reasonableness in unfair dismissal
Key facts	<ul style="list-style-type: none"> • S worked for B on a rota pattern on which employees were not allowed to drink whilst on standby. He raised a grievance at work against his colleagues and an investigation was carried out. • During the course of the investigation comments posted by S were found on his Facebook page that referred to drinking on standby and also used offensive language to describe colleagues. • S was dismissed and brought a claim for unfair dismissal. The tribunal found that the dismissal was unfair as B had not had regard to S's mitigation, such as S's claim that a number of the comments were untrue. B appealed.
Key points	<ul style="list-style-type: none"> • The Employment Appeal Tribunal (EAT) upheld B's appeal, finding that there had been a fair procedure and that B had a genuine belief that S was under the influence of alcohol whilst on standby. • The EAT found that the Tribunal had substituted its own views for that of the employer and had made its own findings of fact about S's actions. Instead the Tribunal should have considered B's views about what had occurred and then assessed whether the dismissal was within the range of reasonable responses. • EAT also commented on the fact the case involved the use of Facebook; it confirmed that such cases are to be determined in accordance with normal principles of law.

Case Name, Citation and Court	Garamukanwa v. Solent NHS Trust (EAT/245/15) Employment Appeal Tribunal
Date	1 March 2016
Subject	Employee's personal emails in a work-related context; right to privacy
Key facts	<ul style="list-style-type: none"> • G was a clinical manager for S and began a campaign of harassment and stalking against another employee, M, which involved sending anonymous emails from email addresses to work colleagues. They had previously been in a relationship. • S carried out a disciplinary hearing and subsequently dismissed G for gross misconduct, having seen the content of the emails. • G claimed unfair dismissal but was unsuccessful, the Tribunal finding that the emails had an effect on work-related matters by affecting M's emotional stability. The decision to dismiss was therefore reasonable and fair. It was held that Article 8 rights had not been engaged. • G appealed to the Employment Appeal Tribunal (EAT), submitting that the emails were private and therefore that S had breached his Article 8 rights.
Key points	<ul style="list-style-type: none"> • The EAT held that Article 8 had not been engaged. Although it said that the aspects of private life could potentially include emails where the sender could expect a degree of privacy, this was very fact dependent. • The EAT emphasised the fact that although the case involved a personal relationship, the issues were brought into the workplace by G's actions. Furthermore, the emails were received by colleagues on work email addresses. • As such it was found that G could have no reasonable expectation of privacy, and even if he did, any interference with his Article 8 rights would have been justified by S's need to protect employee welfare.

Case Name, Citation and Court	<i>Barbulescu v. Romania [2017] IRLR 1032</i> European Court of Human Rights
Date	5 September 2017
Subject	Employer's monitoring of employee's instant messaging account at work; Article 8 right to privacy.
Key facts	<ul style="list-style-type: none"> • S, an employer, requested that B set up an instant messaging account for customer enquiries. B had internal regulations that forbade the personal use of computers but did not indicate monitoring would take place. • S monitored B's communications and alleged a breach of their regulations arising from B making personal use of the computer. S subsequently dismissed B, presenting a transcript of personal messages. • B's challenge reached the Chamber of the ECtHR where he alleged that the dismissal breached his Article 8 right to respect for private life. It was held that whilst Article 8 was applicable, the right to respect for private life had not been violated. B's request of a referral to the Grand Chamber of the ECtHR was accepted.
Key points	<ul style="list-style-type: none"> • The Grand Chamber agreed that Article 8 was applicable, commenting that private should be interpreted in a broad sense, including professional activities. • The court listed a number of relevant factors in relation to the obligation of a State party to protect applicants Article 8 rights (see the Annex for further details). • It was held that the domestic courts had failed to determine whether B had received advance notification of monitoring taking place and failed to have regard to B not having been advised of the nature and extent of that monitoring, or to the degree of intrusion involved. In addition, they failed to determine the employer's reasons for the monitoring and whether the employer could have used less intrusive measures in respect of that aim. • Having regard to all these considerations, the Court found there had been a violation of Article 8.

Case Name, Citation and Court	<i>Antovic and Mirkovic v. Montenegro [2017] ECHR 1068</i> European Court of Human Rights
Date	28 November 2017
Subject	Employer's use of video surveillance at work; Article 8 right to privacy
Key facts	<ul style="list-style-type: none"> • A and M were professors at the University of Montenegro. Video surveillance was introduced in amphitheatres where classes were held, with the aim of improving student safety. • A and M complained to the Montenegro data protection authority for breach of the applicable legislation, and the cameras were subsequently removed. The authority held there was no danger to the people of the auditorium. • A and M then commenced a compensation claim for violation of their right to privacy in the domestic courts. However it was held that, as a public institution, the university was performing activities of public interest and therefore no violation of privacy could take place. • A and M submitted a complaint to the ECtHR that the unlawful installation and use of video surveillance had violated their Article 8 rights.
Key points	<ul style="list-style-type: none"> • The ECtHR held that Article 8 was applicable in the circumstances and noted that it had previously held that 'private life' may include professional activities. • Here, the university theatres were the workplaces of teachers and where professors would interact as well as teach students. • On the facts, it was held that the surveillance amounted to a considerable intrusion into the employee's private life. Furthermore, given that this surveillance was not in accordance with domestic law, the Court found that the interference could not be justified under Article 8(2) ECHR.

Case Name, Citation and Court	Various Claimants v. WM Morrison Supermarket Plc [2017] EWHC 3113 (QB) High Court
Date	1 December 2017
Subject	Employee's online disclosure of other employee's personal information; employer's vicarious liability
Key facts	<ul style="list-style-type: none"> • S, an employee working as an IT auditor, came into contact with the personal details of around 100,000 employees whilst carrying out his role on his work computer. • Having downloaded this data to a USB, he then posted this information online from his home computer. The information was received by a newspaper who informed the employer, M. • M then immediately took steps to remove the data. However, a number of employees brought claims against M. The issue was whether M was directly or vicariously liable for the employee's actions.
Key points	<ul style="list-style-type: none"> • The High Court found in favour of the claimants. • In relation to primary liability under the DPA 1998, M was not the data controller in respect of the posted material and therefore owed no duty to the claimants. Although M had failed to discharge its duty under the DPA to take measures to prevent data loss, this failure did not cause the disclosure. • However, M was held to be vicariously liable as the postings weren't disconnected from S's employment in time, place or nature. M had specifically entrusted S with the payroll data and they had taken the risk in appointing him to the role where he would deal with this data.

Case Name, Citation and Court	Lopez Ribalda and Others v. Spain Applications 1874/13 and 8567/13 European Court of Human Rights
Date	9 January 2018
Subject	Employer's use of video surveillance at work; Article 8 right to privacy
Key facts	<ul style="list-style-type: none"> The five applicants were cashiers working for a supermarket. When the employer noticed stock level irregularities they installed visible surveillance cameras aimed at customers and covert cameras aimed at employees on the checkouts. The five applicants were dismissed for theft. The applicants challenged their dismissals before the Spanish courts, arguing that the use of covert surveillance without notice at work was unlawful. Having been unsuccessful, they applied to the ECtHR alleging that the surveillance violated their Article 8 right to privacy.
Key points	<ul style="list-style-type: none"> The ECtHR held that Article 8 was engaged by the facts and that surveillance of an employee must be considered an intrusion into his or her private life. In installing covert cameras, the employer had not complied with the requirements of Spanish legislation, in that the employees should have been advised as to the personal data that would be processed on them. It was also relevant that the surveillance did not target a substantiated suspicion against the applicants and was on during all working hours. It was held that the employer's interest in protecting its property rights could be satisfied by other means such as informing employees of the installation of a system of video surveillance. As such, it was held that domestic courts had failed to strike a fair balance between the applicants' rights under Article 8 and their employer's interest in the protection of its property rights. There had therefore been a violation of Article 8.

Summary of existing legislation

Introduction

In the UK, there are various pieces of legislation which place different restrictions on employee monitoring. The key acts of legislation are:

- The Data Protection Act 1998;
- The Human Rights Act 1998;
- The Regulation of Investigatory Powers Act 2000; and
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699 (**Lawful Business Practice Regulations**)).

A short summary of the restrictions on monitoring imposed by each is as follows.

Data Protection Act 1998

Employers must comply with the eight data protection principles which include:

- Personal data shall be processed fairly and for specified and lawful purposes (and shall not be processed unless a Schedule 2 condition is met and if sensitive personal data a Schedule 3 condition is also met);
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed;
- Personal data shall be subject to appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage; and
- Personal data shall not be transferred to a country or territory outside the European Economic Area (**EEA**) unless that country or territory ensures an adequate level of data protection.

A minimum requirement of fair processing is provision by an employer of "*fair processing information*" to data subjects outlining the purpose or purposes for which personal data is processed.

At present, many employers rely or purport to rely upon consent under the Act as the basis for the majority of their data processing of employee information, since consent appears as a condition in both Schedule 2 and Schedule 3. It remains common in practice for such consent to be obtained within contracts of employment. The existing view of the ICO is that employers should not rely upon consent as the basis for their data processing and instead should focus on other grounds.

However, such consent obtained within contracts of employment will no longer be valid under GDPR when it is introduced on 25 May 2018 and employers will struggle to rely upon consent going forward. We consider the implications of this in detail below.

Aside from consent, the main condition in Schedule 2 for an employer to rely upon in the context of employee IT monitoring is the "*legitimate interests*" of the employer or a third party. However, this can only be relied upon where those interests are not outweighed in any case by reason of prejudice to the data subject. This ground

and the latest guidance relating to it in the context of employee IT monitoring are discussed in detail below under reference to GDPR, where reliance on legitimate interests will become of importance to the majority of employers.

These existing requirements under the Data Protection Act 1998, taken together, point to the need for employee monitoring to generally be (a) transparent and specified to employees and (b) proportionate having regard to the business aim.

The Employment Practices Code (the **Code**) contains guidance published by the ICO specifically in relation to monitoring at work, including electronic communications. Supplementary Guidance has also been published by the ICO providing more detail by way of guidance. It should be noted the Code is not legally binding but is intended by the ICO to help employers comply with the Act and to encourage them to adopt good practice.

Core principles of the Employment Practices Code include:

- It will usually be intrusive to monitor your workers;
- Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment;
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered; and
- Workers should be aware of the nature, extent and reasons for any monitoring unless (exceptionally) covert monitoring is justified.

In relation to monitoring electronic communications the Code's guidance includes:

- If you wish to monitor electronic communications, establish a policy on their use and communicate it to workers;
- Ensure that where monitoring involves the interception of a communication it is not outlawed by the Regulation of Investigatory Powers Act 2000 (**RIPA**);
- Consider – preferably using an impact assessment – whether any monitoring of electronic communications can be limited to that necessary to ensure the security of the system and whether it can be automated;
- If telephone calls or voicemails are, or are likely to be, monitored, consider – preferably using an impact assessment – whether the benefits justify the adverse impact. If so, inform workers about the nature and extent of such monitoring;
- If emails and/or internet access are, or are likely to be, monitored, consider – preferably using an impact assessment – whether the benefits justify the adverse impact. If so, inform workers about the nature and extent of all email and internet access monitoring;
- Wherever possible avoid opening emails, especially ones that clearly show they are private or personal;
- Where practicable, and unless this is obvious, ensure that those sending emails to workers, as well as workers themselves, are aware of any monitoring and the purpose behind it;

- If it is necessary to check the email accounts of workers in their absence, make sure that they are aware that this will happen; and
- Inform workers of the extent to which information about their internet access and emails is retained in the system and for how long.

At the moment, the ICO has power to fine data controllers up to £500,000 for a breach of the Act.

Individuals can also bring claims for compensation where they have suffered damage or distress arising from a breach of its provisions.

Human Rights Act 1998

The Human Rights Act 1998 incorporates Article 8 of the European Convention on Human Rights into UK law.

This provides "...*everyone has a right to respect for his private and family life, his home and his correspondence.*"

However, this is not an absolute right and may be interfered with under Article 8(2) where such is "*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*"

Public authorities are directly subject to the Act but note that courts and employment tribunals must also, so far as possible, interpret all legislation consistently with the relevant Convention right.

This is important as it indirectly extends the scope of the Act. The practical effect is that an employment tribunal, in determining the fairness of dismissal under section 98 of the Employment Rights Act 1996, must take into account Article 8, if it is considered relevant, in relation to both public authorities and private sector employers.

The case law analysis within this chapter gives a full summary of the relevant cases where both the European Court of Human Rights and the UK domestic courts have considered what Article 8 requires in the context of employee monitoring.

Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA regulates certain types of monitoring, making it unlawful in certain circumstances to intercept a communication in the course of its transmission in the UK.

It applies to the interception of communications in the UK "*by, or with the express consent of a person having the right to control the operation or the use of a private telecommunication system*".

If such an interception takes place "*without lawful authority*" it is actionable by the sender, recipient, or intended recipient if (in the case of a private telecommunications system attached to a public telecommunication system with apparatus in the UK for making that connection) the interception is an "*interception of the communication in the course of its transmission*".

Examples of intercepting in the course of transmission would include the recording of telephone conversations and systems blocking emails and making some of that content available (for example, an offending phrase) to another person.

Opening emails which have already been opened by the intended recipient does not fall within interception in the course of transmission and such monitoring is not subject to RIPA.

If the interception is unlawful under RIPA, the sender, or recipient, or intended recipient would be able to claim damages.

However, an employer will not be liable if it intercepts communications "*with lawful authority*" – that is if permitted either by:

- RIPA itself; or
- the Lawful Business Practice Regulations 2000.

RIPA permits employers to intercept communications where it has reasonable grounds to believe that both the sender and recipient have consented to the interception.

Although obtaining this consent from employees is in theory a possible option for employers (for RIPA purposes only) in relation to internal emails and telephone calls, it is more problematic in the case of external emails, to establish reasonable grounds to believe both sender and recipient consented to the interception.

For that reason, most employers rely instead on the Lawful Business Practice Regulations 2000 to permit interceptions of communications on their systems.

Note also that as discussed below, employers will struggle to rely upon consent under GDPR when it comes into force.

Lawful Business Practice Regulations 2000

These Regulations provide that it is lawful under RIPA for an employer to intercept communications in the course of transmission without consent in order to:

- Ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business;
- Ascertain or demonstrate standards which are or ought to be achieved by persons using the system;
- Prevent or detect crime;
- Investigate or detect the unauthorised use of the system; or
- Ensure the effective operation of the system.

It is also lawful under RIPA for an employer to monitor but not record for the purposes of:

- Determining whether the communications are relevant to the business; or
- Monitoring communications to a confidential anonymous counselling or support helpline.

To rely upon the Regulations, an employer must be able to show that it has made all reasonable efforts to inform every person who may use the telecommunications system that an interception may take place.

Future legislation which may have an impact on employee monitoring

General Data Protection Regulation (GDPR)

The GDPR is the most significant piece of EU legislation which is likely to impact employee IT monitoring. It enters into force in all EC member states on 25 May 2018.

A full analysis of GDPR setting out as it does a comprehensive data protection regime dealing with all aspects of data processing is outside the scope of this report. Instead, we identify below the key features of GDPR which employers will have to take into account in the context of existing and future employee IT monitoring.

It is important to note that the fines that can be imposed (in the UK by the ICO) for a breach of GDPR requirements have been set at a maximum of EUR20 million or 4% of global annual turnover, whichever is greater for the most serious breaches of GDPR, with the lower tier of fines set at a maximum of EUR10 million or 2% of global annual turnover, whichever is greater.

Under GDPR individuals remain able to bring claims for compensation against data controllers arising from breaches of their personal data.

Lawful basis for processing

When processing personal data in the employment context, including within IT monitoring, the data controller must show that one of the lawful grounds for personal data within Article 6 of GDPR is satisfied.

The clear view of both the ICO and the Article 29 Working Party (**WP29**)¹ is that the legal basis relied on by employers should not be consent, due to the imbalance of power within the employment relationship and the requirement that consent be freely given.

The WP29 in its Guidelines on Consent² in fact uses the example of an employer introducing new monitoring technology in the workplace as demonstrating why consent cannot be relied upon:³

"It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in the workplace, or fill out assessment forms, without feeling any pressure to consent. Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of employees (Article 6(1a)) due to the nature of the relationship between employer and employee".

In any event, it should separately be noted also that consent can no longer be relied upon when obtained as one of a number of terms and conditions⁴ (such as is commonly found within employment contracts).

¹ WP29 is an independent European advisory body on data protection and privacy (consisting of representatives of national data protection supervisory authorities) and the leading source of advisory guidance on GDPR

² Guidelines on Consent under Regulation 2016/79, Adopted on 29 November 2017

³ Guidelines on Consent under Regulation 2016/79, Adopted on 29 November 2017, p. 8

⁴ Regulation 7(2)

As such, employee IT monitoring involving the processing of personal data will have to satisfy one of the other lawful grounds within Article 6, such as:

- the processing is necessary for performance of a contract to which the data subject is party;
- the processing is necessary for compliance with a legal obligation to which the controller is subject; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

It seems unlikely that employers will be able to argue that it is necessary to carry out employee IT monitoring in order to perform the employment contract.

Similarly, the situations where an employer can argue that the employee IT monitoring is necessary in order to comply with a legal obligation, may give fairly limited scope for this ground to be relied upon, and will likely be too narrow for most employers.

As such, the vast majority of employee IT monitoring will fall to be justified under the "legitimate interests" ground set out above. The consequence of this should not be underestimated as it is clear that an employer cannot simply state it has legitimate interests in carrying out employee monitoring, for example, in order to protect company data and prevent unauthorised data loss or leakage and then proceed to do so.

WP29 has recently set out guidance to employers in relation to relying upon legitimate interests.⁵ This explains that to be relied upon, the purpose of the processing must be legitimate and the chosen method or specific technology with which the processing is undertaken must be necessary for the legitimate interests of the employer. The guidance further states:⁶

"The processing must also be proportionate to the business needs, i.e. the purpose, it is meant to address. Data processing at work should be carried out in the least intrusive manner possible and targeted to the specific area of risk ... It is essential that specific mitigating measures are present to ensure a proper balance between the legitimate interests of the employer and the fundamental rights and freedoms of employees. Such measures, depending on the form of monitoring, should include limitations on monitoring so as to guarantee that the employee's privacy is not violated. Such limitations could be:

- *Geographical (e.g. monitoring only in specific places; monitoring sensitive areas such as religious places and for example sanitary zones and break rooms should be prohibited);*
- *Data-orientated (e.g. personal electronic files and communications should not be monitored); and*
- *Time-related (e.g. sampling instead of continuous monitoring)."*

The concern of WP29 is that because modern technology enables employees to be tracked over time across workplaces and their homes, through different devices such as smartphones, desktops, tablets, vehicles and

⁵ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017

⁶ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, pp. 7-8

wearables that:⁷

"If there are no limits to the processing, and if it is not transparent, there is a high risk that the legitimate interests of employers in the improvement and efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring."

Practical examples are given within the WP29 guidance specifically relating to IT monitoring which further illustrate the limits of "legitimate interests".⁸

The first example is an employer deploying a Transport Layer Security (**TLS**) inspection service to decrypt and inspect secure traffic with the purpose of detecting anything malicious. However, the application is also able to record and analyse the entirety of an employee's online activity. The legitimate interests are stated to be the necessity to protect the network and the personal data of employees and customers held within that network, against unauthorised access or data leakage.

WP29 recognises these legitimate interests but notes that monitoring every online activity of employees is a disproportionate response and that the employer should first investigate other, less invasive means of protecting the confidentiality of customer data and security of the network.

Suggestions made include configuring the appliance in such a way as to prevent permanent logging of employee activity (for example, by blocking suspicious incoming or outgoing traffic) or so as not to store log data unless it signals the occurrence of an incident.

The second example is an employer deploying a Data Loss Prevention (**DLP**) tool to monitor outgoing emails automatically for the purpose of preventing unauthorised transmission of proprietary data (e.g. customer's personal data). Once an email is considered as the potential source of a data breach, further investigation takes place. The employer relies upon legitimate interests in protecting the personal data of customers as well as the employer's assets against unauthorised access or data leakage.

WP29 states that such a tool may involve unnecessary processing given the scope for "false positives" to arise from legitimate emails, such that the necessity of the DLP tool should be fully justified so as to strike the right balance with the rights of employees.

To rely on legitimate interests, measures should be taken to mitigate the risks such as ensuring that the rules that the system uses to characterize an email as a potential data breach should be "fully transparent" to data users. The suggestion is also made that where the tool recognises an email as a possible data breach that a warning message should inform the sender prior to the transmission, so as to give the option of cancelling it.

Separately, in the context of monitoring home and remote working, WP29 points to the wide availability of technologies that can, for example, log keystrokes and mouse movements, take screen captures (either randomly or at set intervals), log applications used and how long for and potentially enabling webcams. It cautions that the processing involved in such technologies are disproportionate and an employer is very unlikely

⁷ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p. 9

⁸ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, pp. 13-14

to have a legal ground under legitimate interests e.g. for logging keystrokes and mouse movements.⁹

In summary, employers will have to bring any existing and new employee IT monitoring within the limitations of legitimate interests, which will require a balancing exercise to be carried out, weighing up the business interest versus the impact on individual privacy and considering both alternative means and measures which can be taken to lessen the impact, so that the outcome can be shown to be justifiable.

We would recommend that this is documented by way of a legitimate interests assessment (**LIA**) to help demonstrate compliance.

Lawful basis for processing – "special category" data

Under GDPR more restrictive conditions are required to be satisfied in relation to the processing of special category data. This is the new term for what is currently known as "sensitive personal data"¹⁰ under the Data Protection Act 1998, to which GDPR adds two new categories: "*biometric data*" and "*genetic data*".

It is important to note that "*legitimate interests*" cannot be relied upon in relation to the processing of this information. Instead, as well as meeting an Article 6 condition outlined above, there must also be compliance with one of the following narrower grounds within Article 9(2) as well, which include:

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment ... or a collective agreement;
- processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, or medical diagnosis; or
- processing is necessary in the substantial public interest, on the basis of EU or Member State law which shall be proportionate to the aim pursued ... and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

The most likely ground employers will rely upon for their processing of special category data will be the first of these, where the processing of such information is necessary in order to comply with obligations arising from UK employment law. In practice, employers will have to restrict the special category data they hold for these reasons.

In the context of employee IT monitoring, while broadly this should mean that an employer is only holding the special category data it is already permitted to hold, this may not always be the case. An example might be where monitoring of online activity by employees happens to log that a particular employee has carried out internet searches in relation to health symptoms, which they may not have disclosed to their employer and which may not be relevant to their role.

The same point would arise in relation to geo-location tracking technology which might also operate within an

⁹ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p. 16

¹⁰ Information relating to: racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal history or proceedings. Note that criminal conviction data or data about offences under GDPR does not fall within "special category" data but requires an additional condition to be satisfied.

employee's break or personal times, which could record for example the employee visiting a doctors surgery or hospital.

Consideration therefore should be given as to how such special category data relating to the privacy of employees, might be avoided, given the limited grounds an employer needs to satisfy to hold and process special category data.

Privacy Notices

Under the existing Data Protection Act 1998, data controllers must provide specified information, known in the legislation as "*fair processing information*" to data subjects. This currently includes specifying the purposes personal data is used for.

Under GDPR much more detailed information needs to be given to data subjects at the time the personal data is obtained. This includes:

- identity of the data controller;
- purpose of the processing and lawful basis for the processing;
- the legitimate interests relied upon by the data controller or third party, where applicable;
- any recipients or categories of recipients of personal data;
- details of transfers to countries beyond the EEA and legal safeguards taken;
- retention periods or criteria used to determine these periods;
- the existence of each data subject's rights under GDPR;
- the right to withdraw consent (if used);
- the right to complain to a supervisory authority (the ICO in the UK);
- the source of the personal data and whether it came from publicly available sources; and
- the existence of automated decision-making, including profiling and about how decisions are made, the significance and consequences.

Employers will need to prepare detailed privacy notices in advance of GDPR coming into force to communicate this information both to job applicants and existing employees.

In the context of employee IT monitoring, it will be important to ensure there is similar transparency to any data subjects whose communications may be subject to monitoring. This may require, for example, the general privacy notice to refer employees to the more detailed specific policies which provide full details of the nature and extent of monitoring being carried out.

See also the discussion of social media analytics within the section on "*new and emerging technologies*", where failing to advise job applicants that they may be subject to vetting (where there is a lawful ground to do so) will breach these transparency requirements.

Individual rights

GDPR provides for the following rights for individuals:

- The right of access;
- The right to rectification;
- The right to erase;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights in relation to automated decision making and profiling.

This expands on and extends the existing rights contained within the Data Protection Act 1998. The scope of all these rights can be found elsewhere¹¹ but the following points can be made in the context of implementing employee IT monitoring:

- As noted above, privacy notices are required to be prepared advising individuals of their rights under GDPR – we therefore expect to see as a general trend once GDPR comes into force both a growing awareness on the part of employees as to their data protection rights and for them to seek to make use of these rights;
- The right of subject access, which is the most commonly exercised right under the Data Protection Act 1998, may well be used by individuals in future, either as part of general or specific requests, in order to ascertain what information is held on them obtained by employer monitoring. Note that the £10 fee will no longer apply; and
- The right to object to processing applies where the data controller relies upon "legitimate interests" and as such, may be used by individuals in order to challenge what they consider to be excessive monitoring by their employer. Note that where this right is exercised the data controller must stop the processing unless it can show "*compelling legitimate interest*" grounds for the processing which override the interests of the individual.

Automated decisions and profiling

Article 22 of the GDPR gives individuals a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him.

Exemptions apply such as where the processing is necessary for entering into or performance of a contract between the individual and data controller, or where this is required by law, or with explicit consent. However, in the context of employee IT monitoring, the exemptions are likely to have limited application, unless a data controller can point to a legal requirement.

¹¹ See, for example, the ICO's Guide to the General Data Protection Regulation

Except where required by law, individuals have a right where the two other exemptions apply, to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Note that the provisions apply to decisions based solely on automated means, which limits the application of these provisions where a human element still forms part of the decision-making.

See also the discussion of "*big data, artificial intelligence and machine learning*" on "*new and emerging technology*".

Data protection by design and default

Article 25 of the GDPR requires data controllers to implement appropriate technical and organisational measures to show that they have considered and integrated data protection into processing activities. This reflects what has already been good practice recommendations under the Data Protection Act 1998 to place data protection considerations at the forefront of, for example, new HR systems, or in this context employee monitoring technologies.

Under reference to privacy by design, WP29 gives the example of when an employer issues new devices to employees, the most privacy-friendly solutions should be selected, if tracking technology is involved.¹²

Data protection impact assessments

Article 35 of the GDPR outlines the requirements for a data controller to carry out a Data Protection Impact Assessment (**DPIA**) where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing itself, is likely to result in a high risk to the rights and freedoms of natural persons.

Where the DPIA indicates the identified risks cannot be sufficiently addressed by the controller – i.e. residual risk remains high – the controller must consult with the supervisory authority (in the UK the ICO) before commencing processing.

WP29 gives the example of "*systematic and extensive evaluation of personal aspects*" related to individuals based on automated processing and profiling, on which decisions are taken producing legal effects or similarly significant decisions.¹³

Other aspects

The above gives a summary of the main provisions of GDPR that are likely to have implications for employee IT monitoring.

There are also other aspects which may be relevant such as the accountability principle which requires a data controller to be able to demonstrate that they comply with the principles. The tools suggested above such as the LIA, should assist, as part of a wider package of technical and organisational measures that demonstrate

¹² Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p. 8

¹³ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p. 8

compliance.

Staff training and education in relation to GDPR requirements and responsibilities also has a role to play under the accountability principle, and might include specific training on the use of IT systems which highlights the monitoring taking place. This would be consistent also with WP29's view that prevention should be given more weight than detection.¹⁴

Brexit

We do not anticipate that the EU Withdrawal Bill will have any immediate impact on the existing UK restrictions set out in this report. The Bill in its current form is designed to ensure that all directly applicable EU law will be converted into domestic UK law on the date that the UK leaves the EU.

So far as employee monitoring is concerned, the main limitation arises from GDPR which will be included within UK domestic law as at that date. There is to date no sign that the Government intends to take UK data protection in an opposite direction from GDPR; the reverse is true. The Government in publishing the Data Protection Bill noted that it was designed to "*bring our data protection laws up to date*" and will also "*bring EU law into our domestic law*". Also, since international transfers of personal data beyond the European Economic Area require "*adequacy*" to be assured, in order to allow the continuing transfer of personal data with other EU countries, the UK Government is likely to seek a finding on adequacy based domestic law that continues to reflect the key requirements of GDPR.

In relation to The Security of Network and Information Systems Directors (**NIS Directive**) (discussed below) the UK Government's stated intention is that the policy provisions shall continue to apply in the UK.

Where Brexit may have wider consequences, subject always to the final form which Brexit may take, is in relation to future EU law on issues of privacy where future Directives or Regulations would not automatically apply in a post-Brexit landscape.

Investigatory Powers Act 2016

The Investigatory Powers Act 2016 received royal assent on 29 November 2016 but the provisions within the Act which relate to employee monitoring by employers, are not yet in force.

Section 44 of the Act leaves intact the existing position under RIPA 2000 set out above whereby the interception of a communication is authorised if both sender and intended recipient have each consented to the interception. The limitations of this are discussed above hence the reliance placed instead by employers on the Lawful Business Practice Regulations 2000.

The Investigatory Powers Act 2016 (as with RIPA 2000) in its section 46 deals with the interception of communications by businesses for the purposes of monitoring or record-keeping. It provides that the Secretary of State may make regulations authorising conduct by employers of a description specified in the regulations which appear to constitute a legitimate practice reasonably required for the purpose in connection with the activities of monitoring or keeping a record of communications either entering into transactions or relating to the relevant activities or taking place in the course of the carrying on of those activities.

The Government recently consulted in November 2017 over the Act and in particular its obligations in relation to

¹⁴ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p 15

the retention of communication data in light of ECJ case law in December 2016. That consultation closed in January 2018 but the ECJ case law did not extend to data held for business purposes.¹⁵

The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018 have been approved and will be brought into force when s46 of the Investigatory Powers Act 2016 provisions come into force for all purposes. These regulations replicate the existing provisions within the Lawful Business Practice Regulations 2000 and continue the same permitted grounds to monitor employees as exist with the current Lawful Business Practice Regulations 2000.

The Security of Network and Information Systems Directive (NIS Directive)

This Directive was adopted by the European Parliament on 6 July 2016 and requires transposition by EU Member States by 9 May 2018. The UK Government consulted on its plans to implement the NIS Directive in 2017.¹⁶

A key aspect of the NIS Directive is ensuring the framework for the security of network and information systems across sectors which are vital for the economy and society which rely heavily on information networks, such as the energy, transport, water, healthcare and digital infrastructure sectors. Businesses within those sectors which are deemed by Member States to be "*operators of essential services*" will have to take appropriate and proportionate security measures to manage risks to their network and information systems and required to notify serious incidents to the relevant authority. Key digital service providers (search engines, cloud computing services and online marketplaces) will also have to comply with the security and incident notification requirements established under the Directive.

While it will be vital for businesses subject to the Regulations which will implement the NIS Directive to be aware of these additional obligations in relation to security and incident reporting, they do not impose any additional restrictions on employee monitoring in the UK.

ePrivacy Regulation (EC 2016/79)

On 10 January 2017 the European Commission published a draft ePrivacy Regulation with a view to this replacing the current ePrivacy Directive (2002/58/EC). The draft Regulation text has not yet been agreed and it is continuing its legislative progress at EU level. It is aimed at enhancing the protection of privacy and personal data in the electronic communications sector and the scope of the Regulation is extended to all electronic communication service providers.

Although aimed at such providers, in April 2017 the Article 29 Working Party issued an Opinion¹⁷ which indicated that the Regulation required an exception with regard to companies issuing devices or equipment to individuals in respect of the interference prohibition.

Article 8 of the current draft ePrivacy Regulation requires the consent of "*end users*" (e.g. employees) where a party (e.g. employer) wishes to make use of the storage and processing capacities of the end user's equipment

¹⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf

¹⁶ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf

¹⁷ Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 4 April 2017

(e.g. mobile phones, tablets, laptops) and /or collect information from such equipment.

For example, consent from employees will be required to: monitor employees using information from their devices; access the employee's work-related messages or calls on their device; and to update the applications, security features or operating system of their device. Access to work emails may also be subject to consent to the extent that these reside on the device itself and not on the central email server.

This requirement for consent creates a significant problem for employers permitting Bring Your Own Device (**BYOD**). Consent in the context of the employment is generally viewed as invalid and there is no exception included for employers in the ePrivacy Regulations as currently drafted.

The WP29 highlighted this issue in its Guidance on Data Processing at Work (June 2017). It is likely that this point will be subject to further discussion and review before the ePrivacy Regulation is finalised.

France

Commentary on existing case law

- What can we take from this body of case law in relation to employee IT monitoring?

There is a difficult balance to maintain between the right / necessity of the employer to monitor their employees and the proper performance of their employment contract and the employee's freedom and right to privacy even during working hours and at work.

- How important is the case law versus the legislation in placing limitations in these areas?

The legislation mainly imposes limits on the monitoring and restrictions that an employer can impose on employees' rights. Case law is more concerned with the lawful or unlawful nature of evidence used by employers through monitoring to sanction employees.

- Is the reality that the technology is ahead of the legislation with the case law still some way behind and will this continue?

Yes, notably with social media (Facebook, LinkedIn, MSN, etc.). Employees have new ways to express themselves while legislation has not yet integrated these new media.

- How might the key requirements be summarised?

Monitoring must be transparent (with prior notification to employees and staff representatives, if any), fair, not excessive, legitimate and proportionate, and not contrary to employees' right to privacy and freedom.

Trends that can be identified

Case law is adapting existing rules to deal with new forms of communication such as social media (Facebook, etc.). Nevertheless, the same rules apply for other monitoring devices.

Existing case law

List of cases

1. *D v. Instinet France* (page 54)
2. *Société Canon v. X* (n°06-45.279) (page 55)
3. *Sociétés Nouvelles communication téléphonique v. X* (N°11-13-884) (page 56)
4. *Agence du palais v. X* (n°11-19.530) (page 57)
5. *Logidis v. Doyet* (n°12/06776) (page 58)
6. *Newedge group v. GFI* (n°13-14.779) (page 59)
7. *Espace Gestion Bordeaux Girond v. X* (n°14-14.158) (page 60)
8. *Pergam Finance v. X* (n°15-23.522) (page 61)
9. *La grange aux pains v. Mrs U* (n°15-12527) (page 62)
10. *EDSI v. Z* (n°16-12.569) (page 63)
11. *Jesana v. X* (n°16-19.609) (page 64)
12. *Eller Lubrifiants v. X* (n°16-20.618) (page 65)
13. *OPH v. Le G* (n°15-05.739) (page 66)

Case Name, Citation and Court	D v. Instinet France Supreme Court - Employment Division
Date	14 March 2000
Subject	Monitoring employee's phone calls; employee's right to privacy
Key facts	<ul style="list-style-type: none"> • D was employed by Instinet France to make stock exchange orders by phone. He was dismissed by his employer for gross misconduct because he used company devices to gamble. • In court, the employee challenged his dismissal alleging that the company recorded his phone calls, of which he had been informed beforehand, for a purpose other than the reason initially alleged by the employer, namely the justification of the client's order in case of dispute with a client. The employee claimed that the recording of phone calls was thus illicit because used for another purpose.
Key points	<ul style="list-style-type: none"> • The Supreme Court dismissed the claim of the employee. It held that: <ul style="list-style-type: none"> ◦ the employer has the right to monitor and control the activity of his employees during working time; ◦ only the use of secret devices of monitoring is illicit; ◦ the employee was informed in advance of the listening and recording of his phone calls; ◦ the recorded phone calls were valid evidence for the dismissal.

Case Name, Citation and Court	Société Canon v. X (n°06-45.279) Supreme Court - Employment Division
Date	29 January 2008
Subject	Abusive personal use of a company mobile phone by an employee; employee's right to privacy
Key facts	<ul style="list-style-type: none"> • X was employed by Canon and was provided with a mobile phone to perform his employment contract. Canon dismissed him on the ground of abusive use of the mobile phone for personal purpose (63 hours of personal communication in six months). The employer had implemented an auto switch system enabling them to review all communication made by employees and the numbers called. • X lodged an unfair dismissal claim. In defending this claim, X alleged this evidence was illicit because he had not been informed of the auto switch system prior to its implementation, that even during his working hours and at his work place he had a right to privacy and that the employer infringed article 8 of ECHR.
Key points	<ul style="list-style-type: none"> • The Supreme Court dismissed the employee's claim. The mere verification by the employer of the list of numbers called by the employee, their duration, and the costs of the calls was not illicit monitoring merely because the employee had not been informed prior to its implementation. • Since the employee abusively used, during working time, the company mobile phone to make personal calls, his dismissal was justified.

Case Name, Citation and Court	Sociétés Nouvelles communication téléphonique v. X (N°11-13-884) Supreme Court - Employment Division
Date	10 May 2012
Subject	Personal use of the professional computer by an employee; employee's right to privacy
Key facts	<ul style="list-style-type: none"> • X was employed by Sociétés Nouvelles communication téléphonique as a sales person. He was dismissed for gross misconduct due to the inappropriate use of his professional computer because he recorded pornographic pictures and videos of employees without their knowledge. • X lodged an unfair dismissal claim. In defending this claim, X alleged that the pictures and video were on the hardware of his computer in a file named "<i>my documents</i>", so that by opening them, his employer has infringed his right to privacy. • The court of appeal decided that the dismissal was unfair because the pictures were in the file "<i>my documents</i>" and that the employer could not open this file without the presence of the employee without infringing his private life. • The employer appealed against this decision to the Supreme Court.
Key points	<ul style="list-style-type: none"> • The Supreme Court overruled the court of appeal decision; the files were created by the employee with the computer provided by the employer for the performance of his employment contract are by assumption considered work related. The employer can open them without the presence of the employee unless the employee has identified them as personal. The name "<i>my documents</i>" did not, in itself, give a personal nature to the file.

Case Name, Citation and Court	<i>Agence du palais v. X (n°11-19.530)</i> Supreme Court – Civil Division
Date	10 April 2013
Subject	Insulting comments on Facebook accessible only to restricted persons; no public insults
Key facts	<ul style="list-style-type: none"> • X was employed by Agence du Palais and posted offensive comments about her managers on her personal Facebook page and on MSN, accessible only to the individuals who she authorised. • Agence du Palais sued X for damages and prohibition of publication arguing that the comments were public insults. • The Court of Appeal dismissed the claim on the ground that the insults were not public. • Agence du Palais appealed against this decision to the Supreme Court.
Key points	<ul style="list-style-type: none"> • The Supreme Court upheld the decision of the Court of Appeal and dismissed the claim; since the Facebook page was only accessible to authorized persons, which were of a limited number, the comments were not public comments.

Case Name, Citation and Court	<i>Logidis v. Doyet (n°12/06776)</i> Versailles Court of Appeal
Date	13 June 2014
Subject	Video surveillance of employees; employee's right to privacy
Key facts	<ul style="list-style-type: none"> • Doyet was dismissed by his employer because he had been seen on an employer's video surveillance camera stealing the bag of another employee in the company's warehouse. • Doyet lodged an unfair dismissal claim with the Tribunal alleging that the video surveillance was unlawful because he had not been informed of the video surveillance system.
Key points	<ul style="list-style-type: none"> • The Court of Appeal accepted Doyet's claim and held that the dismissal was unfair; the dismissal had been based on the monitoring of employees, however there had been insufficient information communicated regarding these monitoring measures.

Case Name, Citation and Court	Newedge group v. GFI (n°13-14.779) Supreme Court – Commercial Division
Date	10 February 2015
Subject	Employer's right to access mobile phone text messages sent and received by employees
Key facts	<ul style="list-style-type: none"> • Litigation commenced between two broking companies due to the massive poaching by Company A of the employees from Company B, its main competitor. • In the context of the lawsuit, Company B communicated a bailiff-certified report of the text messages on the company mobile phones that B provided to its former employees in order to prove the disorganisation of its business as a consequence of the poaching. • Company A appealed the injunction and opposed the unfair collection of evidence because the former B employees were not informed of the recording and use of their text messages sent and received through the mobile phone put at their disposal by B.
Key points	<ul style="list-style-type: none"> • The Supreme Court rejected the appeal from A; it ruled that text messages sent or received from a mobile phone provided by the employer to the employee in order to perform his employment contract are considered professional and therefore the employer can consult these messages even without the presence of the employee, except if the latter has expressly identified the messages as private. • These text messages can be communicated in court by the employer and are not unfair evidence. • The court held that the use of the text messages by the employer cannot be considered as a recording of a private conversation without employee knowledge.

Case Name, Citation and Court	Espace Gestion Bordeaux Girond v. X (n°14-14.158) Supreme Court – Employment Division
Date	26 January 2016
Subject	Personal nature of files stored on the hardware of the professional computer of the employee and emails from a personal mailbox; employee's right to privacy
Key facts	<ul style="list-style-type: none"> • The employee was dismissed by the employer on the basis of files stored on the hardware of his professional computer to which his employer acceded. • The employer reproached to the Court of Appeal to have dismissed a piece of evidence on the ground that it infringed the correspondence secret. • In an appeal to the Supreme Court, the employer argued that the files and documents created by the employee with the computer put at his disposal by the employer for the performance of his employment contact are by assumption considered professional unless the employee expressly identifies them as personal. • The employer also argued that the files integrated by the employee in the hardware of the computer put at his disposal by his employer are not to be considered as personal merely because they are sent from or to the personal mailbox of the employee.
Key points	<ul style="list-style-type: none"> • The Supreme court upheld the decision of the Court of Appeal; the electronic messages at stake containing the files stored on the computer's hardware came from the personal mailbox of the employee, distinct from the professional mailbox that the employee was using for the performance of her employment contract. • As a consequence, the communication in court by the employer of these emails infringed the employee's right to privacy.

Case Name, Citation and Court	Pergam Finance v. X (n°15-23.522) Supreme Court – Employment Division
Date	1 June 2017
Subject	Admissibility of evidence obtained through an email sent via a professional mailbox without any declaration of the recording system to the French Data Protection Commission (CNIL)
Key facts	<ul style="list-style-type: none"> In litigation regarding a dismissal, the employer communicated emails exchanged between the dismissed employee and its management via the professional mailbox. The dismissed employee argued that the employer did not declare to the CNIL the recording system enabling the employer to record and store the emails and therefore the evidence was not admissible.
Key points	<ul style="list-style-type: none"> The Court rejected the employee's allegation and accepted the evidence. It held that the absence of declaration of the recording system of the professional mailbox, which did not include an individual monitoring of the employee's activity, does not infringe the employee's private life or freedom. As such the communication in court of the emails sent by the employer or the employee via this mailbox was not unlawful because the author of such emails could not ignore that the emails were recorded and stored on the system. The decision of the court may have been different if the messaging system included a system of monitoring of the individual use by each employee of the mailbox, since such a system could infringe the private life and the freedom of employees.

Case Name, Citation and Court	<i>La grange aux pains v. Mrs U (n°15-12527)</i> Paris Court of Appeal
Date	4 October 2017
Subject	Prejudice to employees by pretending to use surveillance at work.
Key facts	<ul style="list-style-type: none"> • An employee was dismissed. • She challenged in court her dismissal and, as an ancillary claim, she alleged that her employer installed an illicit video surveillance system. The employer's response was that these were fake cameras without any video or monitoring capability. • The dismissed employee then requested monetary compensation for breach by her employer of the loyalty obligation, alleging that the employer led the employees to believe that these the cameras were real. As such the employer did not comply with his obligation of information. • In defense, the employer alleged that since the cameras were fake, he was not obliged to inform his employees nor to declare the cameras to the CNIL.
Key points	<ul style="list-style-type: none"> • The Court of Appeal decided that since the cameras were fake, without any recording capability and since the employer did not use any evidence from these cameras, the employer was not obliged to declare them to the CNIL. • Nevertheless, the Court considered that the employer had breached its obligation of information to the employees as these were fake cameras for deterrent purposes. • Thus, the Court held that the employee had suffered a prejudice because she had been misled during the performance of her employment contract.

Case Name, Citation and Court	<i>EDSI v. Z (n°16-12.569)</i> Supreme Court – Employment Division
Date	20 December 2017
Subject	Valid geolocation system; employee's argument of constructive dismissal
Key facts	<ul style="list-style-type: none"> • EDSI implemented a geolocation system to manage the working time of the employees outside of the company's premises, to monitor the use of company cars and for the efficient invoicing of clients. • An employee (Z) sued EDSI in court alleging constructive dismissal because the geolocation was illicitly implemented; it was suggested that another monitoring system could have been used. The employee also argued that as he could use the company car for personal purposes, he should have been able to disconnect the system. The employee alleged that the employer had breached Article 8 of the European Convention on Human Rights and that the use of a geolocation system was a breach of the employment contract justifying constructive dismissal. • The Court of Appeal rejected the employee's claims. • Z appealed against this decision to the Supreme Court.
Key points	<ul style="list-style-type: none"> • The Supreme court dismissed the appeal and held that the geolocation system was not a breach of the employment contract as: <ul style="list-style-type: none"> ◦ the employer organised a meeting to inform the employees before the implementation of the geolocation system; ◦ The employer declared to the CNIL the system; and ◦ The employer informed the employee individually of the geolocation system and its purposes.

Case Name, Citation and Court	Jesana v. X (n°16-19.609) Supreme Court – Employment Division
Date	20 December 2017
Subject	Evidence obtained against an employee through Facebook; employee's right to privacy
Key facts	<ul style="list-style-type: none"> • X was employed by Jesana. Jesana obtained information on X from her personal Facebook page obtained from the professional mobile phone of another employee. • X sued Jesana in court alleging a breach of contract by her employer and constructive dismissal, claiming damages for infringement of her right to privacy. • The Court of Appeal awarded X damages for breach of privacy rights because Jesana used documents posted by the employee on her personal Facebook page and obtained through the professional mobile phone of another employee. • Jesana appealed against this decision to the Supreme Court. Jesana argued that the mobile phone from which it accessed the documents was a professional mobile phone so that all information on this device was, by assumption, professional information, unless the employee had expressly identified the information as personal.
Key points	<ul style="list-style-type: none"> • The Supreme Court dismissed the appeal and upheld the decision of the Court of Appeal; it held that the information from the personal Facebook page of the employee, obtained through the mobile phone of another employee, is a disproportionate and disloyal infringement to the right to privacy of an employee.

Case Name, Citation and Court	<i>Eller Lubrifiants v. X (n°16-20.618)</i> Supreme Court – Employment Division
Date	18 January 2018
Subject	Geolocation of employee - employee's right to privacy
Key facts	<ul style="list-style-type: none"> • X was employed by the company as a sales person. X was subsequently dismissed for poor performance. • X challenged in court his dismissal and requested damages for an illicit geolocation system implemented by his employer. • The Court of Appeal dismissed X's claim with regards to the geolocation because this system was used to justify the dismissal and the employee did not demonstrate the incidence of this system on his work. • X appealed against this decision to the Supreme Court.
Key points	<ul style="list-style-type: none"> • The Supreme Court overruled the decision of the Court of Appeal, stating that an employer cannot impose restrictions on employees that are not justified in relation to the roles performed by employees and not proportionate to the intended purpose of the restriction. • According to the Supreme Court, the use of a geolocation system to monitor the working time of the employees is only licit provided this monitoring cannot be achieved by any other means and provided the employee has been informed beforehand. Such a system is not justified when the employee has independence and flexibility in the organisation of his work schedule.

Case Name, Citation and Court	OPH v. Le G (n°15-05.739) Versailles Court of Appeal
Date	7 February 2018
Subject	Death threats posted on Facebook; employee's right to privacy
Key facts	<ul style="list-style-type: none"> • G, an employee, posted death threats on her Facebook page against OPH employees. A colleague, who was a Facebook friend, captured the Facebook page and communicated it to the employer. The employer dismissed G for gross misconduct. • The employee challenged her dismissal in court.
Key points	<ul style="list-style-type: none"> • The Court of Appeal decided that the employer could not base the dismissal on the comments of the employee on her personal Facebook account; the page was configured to be limited to the employee's friends and to be accessible only to the limited number of people accepted by the employee. • It was held that the fact that one of the Facebook friends was an employee of the employer did not give to the Facebook page a public nature. • In addition, the employer could not prove that the Facebook page was accessible to a large number of its employees.

Summary of existing legislation

In France, the rules regarding employee monitoring are laid down by:

- the French civil code regarding right to privacy and secrecy of correspondence;
- the labour code;
- the French Data Protection Act dated 6 January 1978 as amended; and
- case law.

In summary, the rules are as follows:

An employer has the power to manage and supervise his employees. This implies a disciplinary power and the power to lay down rules necessary for the proper running of the company. Consequentially, employers can monitor and control the activity of employees during working hours and can apply a disciplinary sanction to an employee failing to comply with the company's rules.

Whatever the means or device used to monitor employees, the system must be (i) justified by the nature of the task to be performed and (ii) proportionate the intended purpose (article L.1121-1 of the labour code). This means the monitoring must be legitimate and must correspond to the specific needs of the company.

The monitoring cannot be:

- Secret/disguised: the employer must inform employees of monitoring and the devices implemented in this respect (article L1222-4 of the labour code).
- Unfair: through unfair manoeuvres, trap, stratagem, etc.
- Excessive: accordingly, Supreme court case law and the CNIL prohibit the permanent watch / monitoring of employees at work, except in exceptional circumstances.

The information conveyed to employees in relation to monitoring (except monitoring by their manager or an internal department without any technical device) must occur prior to the implementation of monitoring. The labour code and case law do not lay down any specific approach / means of information. For evidential purposes, it is recommended employers inform employees by a traceable communication (registered letter with acknowledgement receipt or letter delivered by hand against counter signature). The information must be complete and detailed and cover the implemented device, its purpose, the recipient of collected information and the right of the employees to oppose the collection and storage of their personal data.

Failing to comply with these rules will mean the evidence collected through the monitoring will be considered illicit and therefore cannot be used against the employee.

The staff representatives, if any, should be informed and consulted on regarding the implementation of a monitoring device.

Depending on the monitoring device, the company may have to declare the device to the CNIL (subject to the new requirements in the GDPR).

The CNIL also has the ability to check the compliance of companies with the above-mentioned rules and to

impose penalties and other sanctions in case of non compliance.

The monitoring can be made through:

- badge / clock
- video surveillance / camera
- geolocation
- listening and recording of phone calls
- monitoring of mailbox and Internet access

All these monitoring systems must comply with the above mentioned rules. Accordingly, the monitoring device must be intended to check the correct and appropriate performance by the employee of her/his role and cannot exceed this purpose, that is to say cannot infringe the employees freedom and intimacy.

In addition, even during work hours, the employee has a right to privacy and to the secrecy of his personal correspondence. Thus, the employer's right to monitor employees must be weighed against the individual freedom and right to privacy of employees. These freedoms and rights prevent the employer from accessing the personal files / documents of the employee, provided the employee has expressly identified these files / documents as personal.

All files and correspondence sent or received by the employee through the equipment provided by the employer to perform her/his employment contract (computer, mobile phone, company car, etc.) are considered by assumption as professional and thus viewable by the employer, unless the employee has expressly identified them as personal. Indeed, employers cannot prevent employees from having a moderate use of emails for private needs.

Of course, the employer cannot monitor the employees in their private life and while they are out of work, unless their private activity constitutes a breach of their professional obligation (see above-mentioned case law on Facebook use). Indeed, the employee has an obligation of loyalty towards her/his employer.

Future legislation which may have an impact on employee monitoring

The GDPR will impact French law by changing the declaration process towards the CNIL and the necessity for the employer to be proactive in ensuring compliance with the French Data Protection Act.

The development of home office and remote working, notably in the legislation, will also impose new obligations/constraints on the employer (such as the obligation to monitor the working hours of employees and compliance with their professional obligations through an electronic device balanced against respecting the employee's freedom and private life).

No other future legislation is currently being enacted that will impact on employee monitoring.

Germany

Commentary on existing case law

There is a huge amount of case law surrounding employee IT monitoring. The case law listed below reflects a selection of cases relating to video surveillance, monitoring employees' phone calls and email traffic as well as using a private investigator to monitor employees. Proportionality is a common thread of the case law, in particular, balancing the contradictory legitimate interests of the affected parties. These are, on the one hand, the legitimate interests of an employer monitoring their employees in order to prevent criminal offences and/or serious misconduct and to check whether certain policies, contractual/legal obligations and/or certain rules applicable within their business are being observed by the employees. Most case law refers to the employers' fundamental rights to protect the company's financial assets and/ or property rights to ensure proper operational procedures and to remain with those employees who are trustworthy. On the other hand, there are employees' privacy rights, and their legitimate interest in not being monitored while at work to prevent performance pressure and to protect privacy. In Germany there are no specific laws on employees' privacy rights. Such rights derive from the general privacy rights in the German Constitution (*Grundgesetz*) under Article 2 in conjunction with Article 1 which may result in different protected rights, such as the right of information self-determination and the right to one's own image. The provisions deriving from the Federal Data Protection Act (*Bundesdatenschutzgesetz*) apply to the collection, processing and use of employee data. Further specific data protection obligations might follow from applicable works agreements (*Betriebsvereinbarungen*).

Of the cases listed below, it could be outlined that the decisions made by the highest employment court in Germany, the German Federal Labour Court are case specific decisions from which generalisations cannot be made. However, each applicable jurisdiction will consider the principles of proportionality (*Verhältnismäßigkeitgrundsatz*) in all cases of employee IT monitoring. This highlights the importance of considering the following aspects in order to assess whether or not a monitoring measure is permissible:

- the reason behind the monitoring measure (suspected criminal offence or serious misconduct)
- the time and duration of monitoring
- the specific area of monitoring and the reasons for the chosen area (private area or publicly accessible place (e.g. shops))
- monitoring with/without knowledge and/or (explicit) voluntary consent of employees
- the group of affected employees through the monitoring measure
- the specific impact on employees

The case law below shows, inter alia, that the question whether the employers' or employees' legitimate interest are deemed as predominant is only the first question to be answered. A complex follow-up question is whether using the information gathered by the monitoring is permitted in light of the potential breach of privacy rights and/or regulations deriving from the Federal Data Protection Act and/or co-determinations rights of the works council (*Betriebsrat*).

Trends that can be identified

The most recent decision of the German Federal Labour Court - *Bundesarbeitsgericht (BAG)* in 2017 (the decision of German Federal Labour Court dated 27 July 2017 under file number: 2 AZR 681/16) shows that it is difficult to find legal justifications in favor of a (covert) permanent monitoring of employees' behavior and/or performance, especially without any specific reason for the monitoring measure. As an employee's behavior at work can be seen as a part of their privacy rights, covert internal suspicions are unable to legally justify a permanent monitoring in accordance with the Federal Data Protection Act. This is impermissible because of the pressure caused by feeling under constant observation and therefore leads to a considerable infringement of employees' privacy rights.

Even disregarding the validity of the claimed reason for permanently monitoring an employee, e.g. high financial losses shown during inventory, the employer is generally obliged to take the least restrictive action towards their employees that would be effective to achieve the stated goal.

Covert monitoring of employees using technical devices can be permissible under certain limited circumstances, *inter alia*, specific indications of a criminal offence or other serious misconduct by the employee, less restrictive means to find clarifications have been exhausted and that covert monitoring is practically the only remaining and adequate measure to follow.

In accordance with the above, the adherence of the principle of proportionality is a permanent trend which can be found in all cases referring to employee IT monitoring.

Existing case law

List of cases

1. Decision of German Federal Labour Court dated 27 July 2017 under file number: 2 AZR 681/16 (page 73)
2. Decision of German Federal Labour Court dated 20 June 2013 under file number 2 AZR 546/12 (page 75)
3. Decision of German Federal Labour Court dated 19 February 2015 under file number: 8 AZR 1007/13 (page 76)
4. Decision of German Federal Labour Court dated 27 May 1986 under file number 1 ABR 48/84 (page 77)
5. Decision of German Federal Labour Court dated 23 April 2009 under file number 6 AZR 189/08 (page 78)
6. Decision of German Federal Labour Court dated 29 October 1997 under file number 5 AZR 508/96 (page 79)
7. Decision of State Labour Court Hamm dated 10 October 2012 under file number 3 Sa 644/12 (page 80)
8. Decision of State Labour Court Baden-Württemberg dated 22 June 2016 under file number 4 Sa 5/16 (page 81)
9. Decision of German Federal Labour Court dated 13 December 2016 under file number 1 ABR 7/15 (page 82)
10. Decision of German Federal Labour Court dated 27 March 2003 under file number 2 AZR 51/02 (page 84)
11. Decision of German Federal Labour Court dated 29 June 2004 under file number 1 ABR 21/03 (page 86)
12. Decision of German Federal Labour Court dated 21 June 2012 under file number 2 AZR 153/11 (page 87)
13. Decision of German Federal Labour Court dated 22 September 2016 under file number 2 AZR 848/15 (page 88)
14. Decision of German Federal Labour Court dated 25 April 2017 under file number 1 ABR 46/15 (page 89)
15. Decision of German Federal Labour Court dated 20 October 2016 under file number 2 AZR 395/15 (page 90)
16. Decision State Labour Court Berlin-Brandenburg dated 16 February 2011 under file number 4 Sa 2132/10 (page 92)
17. Decision of State Labour Court Berlin-Brandenburg dated 14 January 2016 under file number 5 Sa 657/15 (page 93)

Case Name, Citation and Court	Decision under file number: 2 AZR 681/16 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	27 July 2017
Subject	Monitoring employees via KeyLogger; employee's privacy rights, in particular, the right to informational self-determination (Article 2 in conjunction with Article 1 German Constitution ¹⁸)
Key facts	<ul style="list-style-type: none"> The use of hardware and software for private purposes at the employer's business was prohibited. The employer announced via email to employees the implementation of a new network and that the entire internet traffic and use of the system will be logged and saved in order to prevent any misuse of the internet. No objections were raised by employees. The employer installed software on each employee's (business) computer which enabled the employer to take screenshots of employees' computers and record their keystrokes (KeyLogger). Employee was dismissed without notice (<i>fristlose Kündigung</i>) because he downloaded a computer game and sent emails to his father's logistics company. The claimant lodged a protection against unfair dismissal claim (<i>Kündigungsschutzklage</i>) arguing that his privacy rights were violated as there was no reason for such monitoring. Employer argued that employee's privacy rights were not affected as any non-business-related use of the company's IT systems was prohibited.
Key points	<ul style="list-style-type: none"> The BAG decided that the misuse of the company IT systems was not serious enough to warrant dismissal without notice or to justify an ordinary dismissal. The implementation and use of the KeyLogger constitutes data collection in the meaning of the Federal Data Protection Act (<i>Bundesdatenschutzgesetz-BDSG</i>). The non-objection of employees is not sufficient to comply with the requirements of an employee's approval in the meaning of Section 4a BDSG. Without the employee's approval such use of the KeyLogger tool constitutes a breach of employee's privacy rights regardless of whether the use was conducted openly or secretly. This could not be legitimate under the BDSG as there was no suspected criminal offence (Sec. 32 para 1 sentence 2 BDSG) nor was there any suspected serious breach of obligation (Section 32 para sentence 1 BDSG). Employees' behavior at

¹⁸ In German: Grundgesetz; in the following: "GG"

	<p>work is also a part of his/her privacy rights.</p> <ul style="list-style-type: none">• It can be legally permissible for an employer to openly monitor employees on a random basis to find out whether employees comply with the non-private use of employer's IT systems. This could be done even without a concrete suspicion of a misconduct, however such measures must be adequate and are not allowed to result into a continuous monitoring without any cause.• The BAG accepted that the competent state labour court could not use the defendant's submission of facts referring to the findings from the KeyLogger tool as these findings were made in breach of the privacy rights of employee.
--	--

Case Name, Citation and Court	Decision under file number: 2 AZR 546/12 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	20 June 2013
Subject	Admissibility of evidence gained from a secret search of an employee's locker
Key facts	<ul style="list-style-type: none"> The defendant runs supermarkets. The claimant worked in one of the supermarkets as a sales person. Upon reasonable suspicion that the claimant had stolen merchandise, the store manager opened the claimant's locker in the absence of the claimant but in the presence of a member of the staff association, and allegedly found four items of stolen female underwear. Later, the allegedly stolen items disappeared. The claimant was dismissed without notice for having stolen merchandise, and in the alternative for the strong suspicion of having stolen merchandise. The claimant successfully appealed the dismissal in court, a first decision upheld by the state labour court. The defendant appealed the decision of the state labour court, arguing that the court failed to take evidence concerning the result of the first search of the locker, especially in the form of the witness present at the time of the search.
Key points	<ul style="list-style-type: none"> According to the BAG, the fact alone that a search of an employee's locker was conducted in his absence without his consent may prevent the use of evidence gained in the course thereof in court. The contents of an employee's locker are covered by his privacy rights. The employee thus can trust that his possessions are not searched. A search is nonetheless justified and the use of evidence thus obtained may be justified under Section 32 para 1 sentence 2 BDSG when the employee is suspected of having committed criminal offences. However, in the case at hand, the BAG held that the suspected breach of obligation was not severe enough to grant a secret search of the locker. The employer must first use every means available before conducting a secret search, i.e. the defendant should have asked the claimant to search the locker in his presence. Nevertheless, the BAG declared the appeal founded and referred the case to the state labour court for further fact finding and assessing whether the dismissal may have been justified on grounds of suspicion alone.

Case Name, Citation and Court	Decision under file number: 8 AZR 1007/13 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	19 February 2015
Subject	Monitoring via a private investigator; breach of privacy rights
Key facts	<ul style="list-style-type: none"> Claimant was employed as a secretary. Claimant was incapacitated for work due to a bronchial disease and again later due to a slipped disc. She submitted for a period of two months a total of six medical certificates citing her incapacity to work. The managing director doubted whether the employee was actually unable to work. He engaged a private investigator who monitored the employee for a total of four days, in particular her house, while she and her husband were standing outside their house and while she was visiting a launderette. The final observation letter included 11 pictures, of which nine resulted from video sequences. The claimant lodged a protection against unfair dismissal claim (<i>Kündigungsschutzklage</i>) after receiving notice. The defendant counterclaimed for reimbursement of the costs for engaging the private investigator. The claimant won the case while the defendant lost the counterclaim. Afterwards, she claimed for compensation in the minimum amount of EUR10,500 arguing that the monitoring was illegal and constituted a breach of her privacy rights. The defendant argued the monitoring was permissible as there were various indications for doubting her incapacity of work, e.g. the claimant submitted the first four medical certificates of a general practitioner and only two medical certificates of an orthopedist. The said pictures were taken in public places. No videos were handed over to the employer.
Key points	<ul style="list-style-type: none"> The BAG decided that data being collected by a private investigator via a camera regarding individuals qualifies as personal data collection in the meaning of the BDSG. In order to minimize the evidential value of a medical certificate displaying incapacity to work it is required, at least, to have reasonable doubts regarding such incapacity to work as a criminal offence according to Section 32 para 1 sentence 2 BDSG. The monitoring as well as the covert pictures were assessed as illegal by the BAG as the defendant had no reason for such measure. The BAG accepted the decision by the competent state labour court as regards granting the claimant compensation as a result of serious breach of her privacy rights.

Case Name, Citation and Court	Decision under file number: 1 ABR 48/84 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	27 May 1986
Subject	Works agreement and decision of the conciliation committee ¹⁹ on data collection of employee's phone calls; co-determination rights of works council ²⁰
Key facts	<ul style="list-style-type: none"> The case referred to a works agreement regarding data collection of phone calls made by employees. Each employee had the opportunity to dial "0" in order to define the call as a business phone call as well as to dial "9" in order to define a call as a sole private call. Costs for business phone calls were covered by the employer whereas the employee had to pay for his/her private phone calls. The employer was also allowed to collect data of all outgoing calls, including private calls. The employees challenged the works agreement citing the breach of employees' privacy rights due to the collection of data on the time, date, and the numbers that were called of phone calls made. The employer countered that the respective data collection was necessary to control costs and call manners of the staff.
Key points	<ul style="list-style-type: none"> The BAG decided that data collection of employee's phone calls constitutes personal data of the employee in the meaning of the BDSG; the implementation of such data collection is permitted if such measures are agreed by way of a works agreement or a decision of the conciliation committee which must be in compliance with their regulatory competence and employees' privacy rights; such works agreements are even allowed to deviate from stipulations deriving from the BDSG to the detriment of employees; such works agreement requires the co-determination of the BR in accordance with Section 87 para 1 number 6 Works Constitution Act²¹. The works agreement and decision of the conciliation committee were deemed as valid. In the course of balancing employer's legitimate interests and employee's justified interests, the employer's interest in monitoring and identifying the work performance was held as predominant. The reason for this was that, <i>inter alia</i>, the employees could individually decide to define each call as a private or business call. Therefore, collecting data as to the target number for business calls was allowed where the target number of the defined private calls was not collected.

¹⁹ In German: *Spruch der Einigungsstelle*

²⁰ In German: *Betriebsrat*, in the following referred to as: "BR"

²¹ In German: *Betriebsverfassungsgesetz*, in the following referred to as: "BetrVG"

Case Name, Citation and Court	Decision under file number: 6 AZR 189/08 German Federal Labour Court - <i>Bundesarbeitsgericht</i> (BAG)
Date	24 April 2009
Subject	Admissibility as a witness of someone listening in on a phone conversation
Key facts	<ul style="list-style-type: none"> The claimant worked for the defendant, a temporary employment agency. Due to an accident, the claimant was declared unfit for work by a doctor. On the third day of absence, the claimant received a phone call from the defendant, stating the claimant would face disciplinary action if she did not return to work. One day later, the claimant was dismissed with two weeks' notice. The parties inter alia argued about the exact content of the phone conversation and whether the first dismissal was legal. The claimant argues that – using an unfamiliar phone – the volume was so high that a friend of hers could listen to the whole conversation, something the claimant allegedly wasn't aware of. The claimant further claimed that the defendant asked her to come back to work despite being unfit for work, or else the claimant would be dismissed. The local and the state labour court rejected the claim. The state labour court in particular refused to hear the witness of the conversation.
Key points	<ul style="list-style-type: none"> According to the BAG, privacy rights of a conversation partner are infringed upon when the other conversation partner purposefully arranges for a third party to secretly listen in on the phone conversation. The illicit gathering of such evidence makes its use inadmissible in court: the witness may not give testimony regarding declarations by the other party who is unaware the conversation was being overheard. Reciprocally, where the person adducing the evidence did not contribute to the third party overhearing the conversation, and the latter occurred purely by coincidence, there is no infringement of privacy rights and consequently no prohibition to use such evidence. The BAG accepted the appeal in so far as the state labour court refused to hear the testimony of the witness. Since the third party overhearing the phone call was not necessarily illegal, the state labour court should have enquired whether the claimant intended the witness to listen in or not, and to that end, should have heard the witness regarding the circumstances of the conversation.

Case Name, Citation and Court	Decision under file number: 5 AZR 508/96 German Federal Labour Court - <i>Bundesarbeitsgericht</i> (BAG)
Date	29 October 1997
Subject	Infringement of privacy rights by letting third parties secretly listen in on phone conversations
Key facts	<ul style="list-style-type: none"> The claimant was employed as a prompter at a theatre managed by the defendant (a municipality). Whereas initially the claimant was paid a fixed income laid down in the employment agreement, she was later paid per show only. The parties argued regarding the claimant's remuneration and in particular the contents of a phone conversation she had with the theatre director. The claimant argued that during the phone conversation in question, the director confirmed that the claimant would remain employed for the rest of the season in exchange for the fixed monthly remuneration agreed upon. She also argued that her boyfriend, whom she made listen in on the phone conversation, could testify as to the content of the phone call. The claimant in particular refers to a judgement of the European Court for Human Rights where it was found that not hearing the defendant's former legal representative was a violation of the right to a fair trial under Article 6 para 1 of the European Convention on Human Rights (ECHR).
Key points	<ul style="list-style-type: none"> The BAG found that secretly letting someone listen in on phone conversations is generally not permissible, as it infringes upon privacy rights of the conversation partner. Evidence gathered in that manner is not admissible. Further, the BAG clarified that someone willing to have a third party listen in must advise the conversation partner accordingly. The latter is not obliged to enquire by way of precaution whether anyone else will be listening. Finally, the BAG held that Article 6 para 1 ECHR does not impose hearing the witness who was secretly involved, at least as long as the party who let the witness listen in on a conversation does not provide any significant reason why the listening had to be secret. The claimant could easily have told the theatre director someone else was listening.

Case Name, Citation and Court	Decision under file number: 3 Sa 644/12 State Labour Court Hamm (Westphalia) – <i>Landesarbeitsgericht</i> (LAG)
Date	10 October 2012
Subject	Dismissal for insulting a superior on Facebook
Key facts	<ul style="list-style-type: none"> The claimant was a trainee at a media company offering internet services for companies, run by the defendant. The claimant earnt a low income typical for training contracts. In his private Facebook profile, under the tab “employer” the claimant had inserted the following: <p style="margin-left: 40px;">“oppressor & exploiter Slave ?? Bochum Do stupid shit for minimum wage – 20 %”</p> The defendant dismissed the claimant without notice, giving said Facebook contents as a reason. The claimant successfully challenged the dismissal in court, arguing that the description of his employer was obviously meant sarcastically, did not represent a formal insult, did not mention the name of the defendant nor the company, was covered by the freedom of speech, and finally, that a written warning would have sufficed. The local labour court qualified the statements as insulting, especially since they were aimed at an identifiable person (the employer), yet held against the necessity to dismiss the claimant without notice.
Key points	<ul style="list-style-type: none"> The LAG found that a trainee calling his employer an “oppressor” and “exploiter” and referring to his task as “stupid shit” represented offensive statements that could justify his dismissal without notice, as they suggest that the employer displays a lowly attitude towards employees. The LAG repealed the local court’s judgement and accepted the dismissal as valid. It denied the necessity of a written warning since the breach of obligations was so severe that no positive prognosis about the claimant’s future behaviour could be made.

Case Name, Citation and Court	Decision under file number: 4 Sa 5/16 State Labour Court Baden-Württemberg – <i>Landesarbeitsgericht (LAG)</i>
Date	22 June 2016
Subject	Dismissal for insulting superiors on Facebook by use of emoticons
Key facts	<ul style="list-style-type: none"> The claimant, an assembler working for a mechanical engineering company (the defendant), sustained an injury to his hand that made him unfit for work. On his Facebook profile, a discussion developed regarding his return to work, which involved 21 people including four of his coworkers at the defendant. Extensive use of emoticons was made, with one emoticon representing a pig's head and another representing a bear's head used to refer to two unnamed individuals. Shortly after the defendant learned about the discussion, the claimant was dismissed without notice. The defendant argued that it was obvious from the context of the discussion that two of the claimant's supervisors and colleagues were being insulted as animals. The claimant challenged the dismissal as unfounded, arguing that the communication on Facebook was private and understandable only to insiders. Further, he presented further explanation according to which the animal heads referred to a colleague participating in the discussion and to his own nickname "bear". The local court held in favour of the claimant, judging that after 16 years of irreproachable employment an immediate dismissal seemed inappropriate.
Key points	<ul style="list-style-type: none"> The LAG held that insulting superiors on Facebook by using emoticons in a colleague's comment function indeed may justify a dismissal. This will in any case require the extensive balancing of interests. Regarding the case at hand, the LAG assumed that the comments were indeed insulting. However, the LAG found that a written warning instead (instead of a dismissal) would have been enough to prevent the claimant from repeating such offensive comments. In particular, the LAG took into account that the claimant probably was acting under the false assumption that only a limited circle of persons would take notice of the comments, and that dismissing him would put him in an extremely difficult social and financial situation.

Case Name, Citation and Court	Decision under file number: 1 ABR 7/15 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	13 December 2016
Subject	Social media and co-determination of group-wide works council ²² on the implementation and use of an employer's Facebook page
Key facts	<ul style="list-style-type: none"> • The employer, a controlling company of a group offering blood donation services, had approximately 1300 employees in the group. Approximately 40 appointments of blood donations were executed with numerous medical doctors and further employees. The employer and the works council decided on a IT group-wide frame works agreement (IT-KBR). The employer set up a Facebook page to display a unified presentation to the group. The internet-based software was provided by Facebook and enabled registered users to deliver guest posts visible to all visitors to the Facebook page. The Facebook page was administered by a group-wide group of approximately 10 employees who provided the page with posts and comments and who could delete certain posts. A user posted a complaint on placing an injection needle, while another user was complaining about a lack of regular check-up prior to the blood donation. • The works council complained that the Facebook page was implemented and used without the required co-determination of the works council in accordance with Section 87 para number 6 BetrVG as a certain function called "<i>graph search</i>" would enable for the employer in future (and also in German language) to collect data on employees' behavior. The performance of the employee's group being responsible for the administration of the Facebook page are electronically collected and saved. The visitors' posts regarding the behavior and performance of employees are visible to an unlimited group of individuals without prior control by the employer. The employer countered that the IT-KBR already covers the implementation and use of the Facebook page. No data as to the behavior and performance of employees are collected nor processed. The group of employees being responsible for the Facebook page use a general administration login which does not allow recognition of who posted information. The received information by the visitor postings are not collected by the employer.

²² In German: *Konzernbetriebsrat*; in the following referred to as: "**KBR**"

<p>Key points</p>	<ul style="list-style-type: none"> • The BAG decided that the functions currently provided by Facebook with respect to data evaluation options (e.g. “like” button) does not qualify for monitoring of employee’s behavior and performance as the functions do not lead to individualized judgements on employees. The group of employees responsible for the administration of the Facebook page do not qualify for technical facilities pursuant to Section 87 para 1 number 6 BetrVG as it is not possible to determine which individual posted on the group due to the general administration login. • Likewise, the BAG decided that the function enabling the Facebook user to make “posts” on their page is subject to co-determination right of the KBR in accordance with Section 87 para 1 number 6 BetrVG as the Facebook page qualifies for such technical facilities. Some postings allowed certain comments to be assigned to employees. In such cases the employer can monitor behaviour and performance of the employees which results in the privacy rights of employees being affected and lead to a performance pressure for employees. • As a result, the employer had to change his Facebook settings by deactivating the function which allows <i>“postings of other users on the Facebook page”</i>.
--------------------------	--

Case Name, Citation and Court	Decision under file number: 2 AZR 51/02 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	27 March 2003
Subject	Secret video monitoring of an employee; exclusion of evidence; privacy rights
Key facts	<ul style="list-style-type: none"> The claimant had been employed as a cashier from 1994 at the employer, a company running a store with beverages market. In 1997, it was identified that inventory was missing. The defendant installed, in March 2000, a video camera directly over the cash desk, followed by another camera being installed in September 2000 to monitor the corridor of the beverage market. The assessment of the video monitoring of five days led to a suspected embezzlement. The claimant was in charge on all five days. After confronting the claimant with the video material in the presence of two works council members the claimant was dismissed without notice. The BR approved the dismissal. The claimant lodged a protection against unfair dismissal claim (<i>Kündigungsschutzklage</i>) disputing to have committed any criminal offence. Further, she argued that the video material must be excluded as evidence because these were made in breach of her privacy rights. The defendant countered that first suspicion moments against the claimant arose in July 2000 during the video monitoring. Other possible measures (e.g. review of merchandise management system) lead to the assumption that only an employee's misconduct at the cashier desk could be the source of errors. Therefore, installing the video camera was unavoidable. The BR approved installing the video cameras secretly. The employment court dismissed the case, followed by the same decision by the state labour court.
Key points	<ul style="list-style-type: none"> The BAG decided that the dismissal without notice was valid based on the suspicions of criminal offences by the defendant. Although it was decided that the secret video monitoring of employees qualifies for a breach of privacy rights in accordance with Article 2 para 1 GG. Such breach is justified if legitimate interests of the employer are deemed as predominant. Such breach does not result into the exclusion of evidence if there was a concrete suspicion of a criminal offence or another serious misconduct to the detriment of the employer and if no less restrictive means of achieving the clarification are given, i.e. the secret monitoring was the only remaining measure and not disproportionate in total. The non-compliance with co-determination rights of the BR does not result

	into an independent exclusion of evidence provided the BR approved the use of the evidence and the dismissal and the use of evidence is justified in accordance with general principles. Restrictions deriving out of Section 6 b BDSG for video monitoring in publicly accessible places came into effect in May 2001 and were not applicable here.
--	--

Case Name, Citation and Court	Decision under file number: 1 ABR 21/03 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	29 June 2004
Subject	Video monitoring of the work place and principles of proportionality
Key facts	<ul style="list-style-type: none"> The defendant realized there were a huge amount of lost mailings based on reported losses and on estimated number of unreported loss cases. The employer decided to install a monitoring system of cameras in order to prevent mailing losses and criminal offences and to help investigate criminal offences. The employer did not receive the BR's approval. The decision made by the conciliation committee enabled such monitoring measure with, inter alia, video monitoring of 50 hours per week. The BR challenged the decision in front of the local court arguing that such measure without any specific reason is inadequate and unnecessary to prevent, clarify and investigate on potential criminal offences. The employment court dismissed the case, the same decision was repeated by the state labour court. The BAG denied the formed decisions and held the decision of the conciliation committee invalid.
Key points	<ul style="list-style-type: none"> The implementation of monitoring working places with a video camera is subject to BR's co-determination right pursuant to Section 87 para 1 number 6 BetrVG. The overall circumstances are crucial in order to comply with the principles of proportionality, i.e. the specific measure must be suitable and necessary in order to achieve the envisaged goal. The affected restrictions and the envisaged goal must be balanced adequately. According to the BAG the implementation of video monitoring constituted a serious breach of Section 75 para 2 BetrVG. The employees' legitimate interests were qualified as predominant due to the severity of the impacts (e.g. permanent monitoring without any concrete initial suspicion, high performance pressure). According to the BAG there were other less restrictive measures possible (e.g. checking employees' bags when leaving the working place, TV monitoring) than permanent video monitoring.

Case Name, Citation and Court	Decision under file number: 2 AZR 153/11 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	26 June 2012
Subject	Secret video monitoring; privacy rights of employees, exclusion of evidence
Key facts	<ul style="list-style-type: none"> The employer runs a business in the retail industry. With the approval of the competent BR the employer installed video cameras in the shop in December 2008. During the data evaluation in the presence of a works council member the employer found out that the employee secretly stole cigarettes. After consulting the BR the employer dismissed the employee without notice in January 2009. The claimant lodged a protection against unfair dismissal claim (<i>Kündigungsschutzklage</i>) arguing that the secretly collected video material could not be used as evidence as these were made in breach of her privacy rights. The defendant (employer) countered that the employee committed a criminal offence. The secret video monitoring was necessary as the business suffered high inventory losses (approx. EUR 7,600 on a monthly basis). There were, additionally, suspicions of theft by the staff which would have immense influence on the inventory differences. The employment court dismissed the case, the state labour court decided that the ordinary dismissal was socially justified as a criminal offence to the detriment of the employer constitutes serious misconduct by employee. The BAG held the revision of the case lodged by the employee as justified and decided that it still must be decided by the state labour court whether an exclusion of evidence is given here due to the breach of privacy rights of the employee.
Key points	<ul style="list-style-type: none"> Section 6b para 2 BDSG requires the video monitoring to be visible in publicly accessible places. However, evidence collected through secret video monitoring does not constitute for an independent exclusion of evidence if such data were collected in breach of Section 6b para 2 BDSG. Secret video monitoring of an employee can be permissible if a concrete suspicion of a criminal offence or another serious misconduct to the detriment of the employer towards a, at least, spatial and functional definable group of employees is given and less restrictive means of achieving clarifications as to the concrete suspicion were exhausted without result, i.e. the video monitoring results in being the only remaining means which is not disproportionate.

Case Name, Citation and Court	Decision under file number: 2 AZR 848/15 German Federal Labour Court - <i>Bundesarbeitsgericht</i> (BAG)
Date	22 September 2016
Subject	Video surveillance of employees at their workplace due to suspected theft; use of evidence found by chance
Key facts	<ul style="list-style-type: none"> The defendant, a food retail company, noticed in a specific store a ten-fold increase of merchandise unaccounted for compared to the previous stock-take. After further inquiry, the defendant held employees responsible, but inspections and control measures were inconclusive. The defendant secretly conducted video-surveillance of the checkout area, justifying it with the suspected theft by two employees. The so far unsuspected claimant, an employee working as deputy store manager and cashier, was filmed manipulating the pay machine, pretending that 13 returnable bottles had been returned, and taking for herself the amount of deposit for 13 bottles. Having been dismissed without notice, the claimant lodged a protection against unfair dismissal claim (<i>Kündigungsschutzklage</i>). The local court held in the claimant's favour, whereas the state labour court repealed the claim. The BAG confirmed the state labour court's decision.
Key points	<ul style="list-style-type: none"> The BAG held a chance find stemming from covert video-surveillance justified under Section 32 para. 1 sentence 2 BDSG aimed at another suspected criminal behaviour may also be used as evidence in court against a previously unsuspected person for a different criminal behaviour. Further according to the BAG, where video-surveillance is justified under Section 32 para. 1 sentence 2 BDSG, employees need not be informed of the secret surveillance. Data protection provisions do not prevent the use in labour law cases of data collected in breach of said provisions. Where the use of such evidence infringes upon a party's privacy rights, this is justified only where there is an legitimate interest going beyond the gathering of evidence. This, the BAG held, was the case here, where substantial abuse of confidence was being investigated.

Case Name, Citation and Court	Decision under file number: 1 ABR 46/15 German Federal Labour Court - <i>Bundesarbeitsgericht (BAG)</i>
Date	25 April 2017
Subject	Co-determination rights of BR regarding implementation of load statistics
Key facts	<ul style="list-style-type: none"> The employer is an insurance company with 38 sites in Germany handling damages. Each site is represented by a field executive. All consultants at the sites are summarized into a group which is organized by a group leader. The work load of the consultants is defined through phone activities, mail inbox and damage management. After the employer and the works council could not reach an arrangement on implementing load statistics through IT systems a decision was made by the conciliation committee. The decision enabled a comprehensive monitoring of employees' work performance and behavior by way of a detailed concept of indicators and thresholds. The BR challenged the decision arguing that it constitutes a breach of privacy rights of all employees according to Section 75 para 2 BetrVG. The employer countered that no outstanding monitoring pressure would arise as there was personally restricted access and use of the employees' data. The employment court dismissed the case and the state labour court confirmed the said decision. The BAG denied the decisions and held the application of the BR as justified.
Key points	<ul style="list-style-type: none"> A works agreement on load statistics enabling assessment of crucial parts of employees' working behavior with quantitative criteria constitutes a serious breach of employees' privacy rights. Such breach cannot be justified by the legitimate interests of an employer to analyze the load situation to improve productivity. The co-determination rights of the BR pursuant to Section 87 para 1 number 6 BetrVG shall protect employees from breaches of their privacy rights by way of technical facilities which are justified and not disproportionate.

Case Name, Citation and Court	Decision under file number: 2 AZR 395/15 German Federal Labour Court - <i>Bundesarbeitsgericht</i> (BAG)
Date	20 October 2016
Subject	Secret monitoring; dismissal without notice
Key facts	<ul style="list-style-type: none"> The employer, a car dealer, employed the claimant in 1979 as a motor mechanic. The employer had a factory spare parts warehouse which was administered by two employees and to which all employees had access to until 2013, i.e. the employees were allowed to take out spare parts to sell or fit them to cars. The employer realized losses of spare parts in November 2013 and February 2014 during an inventory. These differences were made public to the staff. The employer prohibited the access to the factory spare parts warehouse except for the two employees administering the warehouse. After further inquiries did not lead to clarifications, the employer installed a video camera enabling the monitoring of the spare parts warehouse. Only the two responsible employees and the plant manager were aware of this measure. The BR was not consulted. The monitoring showed the claimant entering the factory spare parts warehouse and putting a package of brake blocks into his pocket. After confronting the claimant with the video material the employer dismissed the employee without notice based on (suspected) criminal offence. The claimant lodged a protection against unfair dismissal claim (<i>Kündigungsschutzklage</i>) disputing to have committed any criminal offence. Further, the claimant argued that the video monitoring material were made in breach of BDSG regulations and co-determination rights of the BR which must lead to the exclusion of evidence. The defendant (employer) countered that the video monitoring took place at a time when the employer had reasonable suspicions relating to criminal offences committed by the staff. The storehouse keeper approved the monitoring of their working places. The video monitoring of the claimant took place due to the fact that the claimant ignored the access prohibition. The employment court and state labour court held the case as justified. The BAG decided to reject the claim to the state labour court. According to the BAG the state labour court decided wrongfully to exclude the video monitoring material as evidence based on the fact that it was made in breach of privacy rights.
Key points	<ul style="list-style-type: none"> The collecting, processing and using of personal data in order to investigate on criminal offences in the meaning of Section 32 para 1 sentence 2 BDSG

	<p>requires a simple suspicion in the meaning of an initial suspicion which must be more than vague indications and mere speculations. However, findings obtained or evidence delivered in breach of such regulations does not result in an exclusion of such findings or evidence in the course of a employment litigation case.</p> <ul style="list-style-type: none">• Secret video monitoring of an employee can be permissible if a concrete suspicion of a criminal offence or serious misconduct to the detriment of the employer is given, and less restrictive means of achieving clarification as to the concrete suspicion were exhausted without result, i.e. the video monitoring in being the only remaining means which is not disproportionate. According to the BAG the said prerequisites were fulfilled in this case.
--	--

Case Name, Citation and Court	Decision under file number: 4 Sa 2132/10 State Labour Court Berlin-Brandenburg – <i>Landesarbeitsgericht (LAG)</i>
Date	16 February 2011
Subject	Employer access to employee emails sent via company email system
Key facts	<ul style="list-style-type: none"> According to the defendant's email policy, employees may use the company email for private purposes with their superior's consent, provided such emails are marked as "private". A limited control of such use requires suspected abuse, the data protection officer's consent and informing the staff council. The content of private emails may only be reviewed with the employee's consent, or where initiated by law enforcement authorities. Another company guideline provided that all employees must arrange for their emails to remain accessible to a replacement during absences. The claimant, who worked in the defendant's customer support, used her company email privately. In view of a planned absence, she deactivated the replacement setting. She fell ill during the planned absence, with no one else having access to her emails. After two months of absence, the defendant had the claimant's account opened and all business related emails printed for further processing. The claimant filed for an injunction to prevent her employer from further accessing her email account or forwarding any incoming emails without her consent. She argued that the defendant, in providing her with such an email system, is a service provider under the German Telecommunication Act (<i>Telekommunikationsgesetz</i>) and as such under the obligation to respect the secrecy of telecommunications. She also accused the defendant of criminal offences under Sections 202a and 206 German Criminal Code (<i>Strafgesetzbuch</i>) relating to data secrecy. Her claim was dismissed by the local court and the appeal rejected by the LAG.
Key points	<ul style="list-style-type: none"> The LAG held that the company does not qualify as a service provider. The secrecy of telecommunications only applies to the communication process, whereas the defendant intervened only once the communication process (transmission and reception of emails) was completed. An infringement of privacy rights, had it occurred (denied by the LAG), would have been justified, given the claimant's lack of compliance with the replacement system and the need to ensure proper customer support.

Case Name, Citation and Court	Decision under file number: 5 Sa 657/15 State Labour Court Berlin-Brandenburg – <i>Landesarbeitsgericht (LAG)</i>
Date	14 January 2016
Subject	Dismissal without notice due to excessive private use of the internet at work
Key facts	<ul style="list-style-type: none"> The employer provided an internet connection to his staff. The employees were only allowed to use the internet for private purposes in exceptional cases and only during break time. The employer received information on a misuse of the internet by the claimant. The claimant worked on a weekly 40 hours basis for the employer. Following this information the employer started evaluating the internet browser history of the employee's business computer. The employee found out that the claimant used the internet for private purposes for approximately 40 hours during a period of 30 days. The employer dismissed the employee without notice after consulting the BR. The claimant lodged a protection against unfair dismissal claim (<i>Kündigungsschutzklage</i>) arguing that the private use of the internet was explicitly allowed and complaining that the evaluation of the data were made in breach of his privacy rights. The employment court dismissed the case and the State Labour Court of Berlin-Brandenburg confirmed the decision by stating that the dismissal without notice was valid in accordance with Section 626 German Civil Code.
Key points	<ul style="list-style-type: none"> An exclusion of evidence in virtue of Section 88 para 3 Telecommunications Act²³ was denied as this law is not applicable if the employer grants the private use of the internet connection at work because the employer cannot be qualified as a service provider in the meaning of the TKG. Excessive private use of the internet at work amounting to approximately 40 hours during the working hours within a period of 30 days authorizes the employer to dismiss without notice, even if the employer allowed the private use of the internet in exceptional situations within break time. In order to evidence an excessive private internet use, the employer is allowed (without approval of the employee) to collect and evaluate such data from chronicles of the internet browser which was installed on the business

²³ In German: *Telekommunikationsgesetz*, in the following referred to as: "TKG"

	<p>computer of the employee. Section 32 para 1 sentence 1 BDSG allows such collecting and evaluating in order to prevent misuse.</p> <ul style="list-style-type: none">• The appeal to the BAG was permitted due to the fundamental meaning of the case. The BAG has yet not decided on the case.
--	---

Summary of existing legislation

Introduction

In Germany, there are various pieces of legislation which place different restrictions on employee monitoring. Without any claim to completeness, the key acts of legislation are, from our perspective, the following:

- The German Constitution (*Grundgesetz-GG*)
- The Federal Data Protection Act (*Bundesdatenschutzgesetz-BDSG*);
- The Telecommunication Act (*Telekommunikationsgesetz-TKG*)
- The German Criminal Code (*Strafgesetzbuch-StGB*)
- The Works Constitution Act (*Betriebsverfassungsgesetz-BetrVG*)

A short summary of the restrictions on monitoring imposed by each is as follows.

The German Constitution (*Grundgesetz-GG*)

The German Constitution grants a general right of privacy. Employees working in Germany, regardless of their nationality and/or citizenship, are therefore protected by the general right of privacy enshrined in **Article 2 para1 in conjunction with Article 1 para 1 GG** as the so called *Allgemeines Persönlichkeitsrecht*. The *Allgemeines Persönlichkeitsrecht* is a fundamental right in the German Constitution. As such the fundamental rights of informational self-determination (*Recht auf informationelle Selbstbestimmung*) and the fundamental rights to one's own image (*Recht am eigenen Bild*) are significant manifestations resulting from the general privacy rights. Moreover, there is also protection for the spoken word, i.e. the right to determine on your own whether the spoken word is available to the partner of the conversation only or also made accessible to third parties or even the general public, and whether it may be recorded by electronic or other means.

In accordance with the jurisdiction of the German Federal Constitutional Court (*Bundesverfassungsgericht*) the right on informational self-determination preserves for every individual the right to decide on their own on the surrender and use of personal data as a basic principle. The right to one's own image grants for every individual the right to decide on their own as a basic principle if and to which extent others may publically present their biography or certain events of their lives. As such the right to one's own image is also a right deriving from the right to self-determination. The need for protection, results from the possibility of using an individual's personal, private data and distributing it to the public. Infringements of the aforementioned rights can only legally be deemed as justified if, *inter alia*, the above mentioned principle on proportionality (*Verhältnismäßigkeitsgrundsatz*) is observed in each specific case. Monitoring measures decided and undertaken by an employer regularly lead to a conflict with employees' general privacy rights. Therefore, any monitoring measures which may lead to the violation of employees' general privacy rights must be in compliance with the principle on proportionality. This implies that legally legitimate interests of the employer must be weighed against the employee's general privacy rights.

The Federal Data Protection Act (Bundesdatenschutzgesetz-BDSG)

Pursuant to the current BDSG the collection, processing and use of personal data can only be deemed as valid if a statutory provision allows or prescribes it or if the individual has consented to this.

In accordance with **Section 32 para 1 sentence 1 BDSG** the employer is allowed to utilize personal data of employees if the usage of the respective data is necessary for the establishment or performance or termination of an employment relationship. The said provision requires that the collection and processing of all personal information happens due to the "*purpose of the employment relationship*". E.g. data such as name, address, bank details, sex and works council membership are important for the establishment and administration of the employment relationship. Data such as language skills, schooling and family status are important for personnel planning. Further, data such as sickness and time of absence are important as a performance measurement.

Section 32 para 1 sentence 2 BDSG authorizes the employer to process and use employee's data to unveil criminal actions by the employee. In this regard, the following prerequisites must be fulfilled:

- there is actual evidence which causes suspicion that the employee has committed a criminal offence in the framework of the employment relationship;
- the processing and use of the data is necessary for the purpose of prosecuting the crime; and
- no other overriding legitimate interest of the employee in his data being excluded from such processing and use is given.

Apart from the abovementioned, personal data of employees can also be legally utilized by obtaining the employee's consent pursuant to **Section 4a BDSG**. The consent must be based on a free decision and the employee must be informed on the purpose of the collection, processing and use of the data. Additionally, the employer has to point out the consequences that may occur if consent is not given provided that the employee requests this or in so far as the circumstances of the individual case require such information.

Such consent shall be generally given in writing unless there are specific circumstances allowing for any other form of communication. If such consent is given simultaneously with an agreement of other matters the declaration of consent must be highlighted specifically so that the employee's attention is drawn to the declaration. If the consent includes special types of personal data the consent needs to refer explicitly to these special types.

Please note the following: regarding the language of the consent; there are no specific requirements apart from the requirement that the data subject is able to read and understand the respective provision. E.g. if all employees are capable of reading and understanding English, no German translation would be required.

There is, furthermore, a general discussion between some commentators in the field of the legal literature doubting whether an employee's data privacy consent within employment agreements can be qualified as voluntary due to the fact that there is a general subordination relationship between employer and employee. Based on this, only in special cases is such consent recommended. If such consent is stipulated in an employment agreement, special relevance shall be given to it, e.g. by typing the provision in bold letters.

With respect to surveillance of premises open to the public, e.g. salesrooms, video monitoring must exercise the householder's rights or a legitimate interest to follow specifically determined purposes (**Section 6b para 1 sentence 2 Nr.2/3 BDSG**). Such surveillance and the responsible authority must be made visible to the public

by way of appropriate measures.

In contrast to the above, the covert surveillance of workplaces with restricted access may be authorized on the basis of **Section 32 BDSG** in accordance with strict prerequisites in accordance with the Federal Labour Court.

Please also note that works agreements regarding the processing and use of employee's data constitute statutory provisions within the meaning of the BDSG. Based on this, works agreements may include the utilization of employees' data to the advantage of the employer and the data protection safeguards of the works agreement may differ from the statutory provisions. However, the protection standard deriving from such works agreements shall not fall considerably below the statutory standard and the employer, like a works council, is obliged to safeguard and promote development of personality of the employees in the company (Section 75 para 2 Works Constitution Act).

The infringement of certain regulations stipulated in the BDSG can legally lead to an administrative offence and/or a criminal offence pursuant to **Section 43 and Section 44 BDSG**. E.g. video monitoring can be qualified as collecting personal data. Based on this, the employer can be subject to a fine (*Geldbuße*) which can be imposed by the competent authorities pursuant to **Section 43 para 2 BDSG** provided such video monitoring happens with intent or negligence by the employer in an unauthorized way. Such fine could currently amount to a maximum of EUR30,000. Under certain circumstances such unauthorized data collection can also qualify for a criminal offence pursuant to **Section 44 BDSG** if the action in the aforementioned sense is made intentionally and in exchange for money or in order to enrich yourself or another or in order to harm another. If certain prerequisites are fulfilled an imprisonment of up to two years or a financial penalty can result.

The Telecommunication Act (Telekommunikationsgesetz-TKG)

If an employer allows the private use of internet and/or email in the work place the employer could be qualified as a service provider in the meaning of **Section 88 TKG** with the consequence that he is bound to the telecommunication secrecy obligation deriving from that provision. This can also lead to the data protection secrecy provisions of the TKG to apply to private email and internet use. These provisions severely restrict the access and permanent monitoring of private emails and internet communication.

It is predicted that conflicts between data protection laws will occur as it can be difficult to determine which communication belongs to the business use of internet and email and which communication is private. The legal situation is currently unclear on whether an employer qualifies as a service provider in such a scenario. Therefore, in most cases it is recommended that the employer prohibits the private use of the internet and email at work and consequently takes care that such prohibition is adhered to by the staff. Therefore potential conflicts with the TKG are avoided.

The German Criminal Code (Strafgesetzbuch-StGB)

The use of telecommunication systems at work may lead to a collision of employees' and employer's legitimate interests. With respect to monitoring measures undertaken by the employer, statutory restrictions can also derive from the German Criminal Code, specifically related to the following criminal offences: **Section 201 StGB** (violation of the privacy of the spoken word), **Section 202 StGB** (violation of the privacy of the written word), **Section 202b** (phishing), **Section 206 StGB** (violation of the postal and telecommunication secret). If the specific prerequisites are given in a certain case then imprisonment or a financial penalty can be imposed by the competent authorities.

The Works Constitution Act

The monitoring of employees triggers a co-determination right by the works council pursuant to **Section 87 para 1 number 6 BetrVG**. The works council has a right of co-determination especially in the event of the introduction and application of technical systems which are suitable for monitoring the conduct or performance of the employee. Based on this co-determination, rights should be observed if a works council exists at the respective company.

Future legislation which may have an impact on employee monitoring

The European General Data Protection Regulation (**GDPR**) may have an impact on different restrictions on employee monitoring. In this regard we refer to the comments made under the United Kingdom section of this report.

The new version of the (German) Federal Data Protection Act will be effective as of 25 May 2018 and will replace the current version of the BDSG.

Spain

Commentary on existing case law

Spanish case law has been debating IT monitoring for a long time, weighing employees' rights (information, consent, secrecy of communications and dignity) against the employer's organizational power (Article 20 of the Employment Act). In this sense, case law regarding IT monitoring can be summarized, in one sentence, as follows: monitoring measures by the employer must be suitable, proportionate and necessary, and the employee must be aware of them.

Bearing in mind the above, under Spanish law, monitoring employees is lawful. However, such control is not absolute. To understand if a Fundamental Right has been breached, a case by case assessment must be undertaken. In this sense, it must be evidenced whether the monitoring measure is proportional and suitable.

In addition, it is essential to highlight the organisational role of the employees' representatives within the monitoring process. Representatives must be duly informed about the company's monitoring measures, for example, the employees and their legal representatives must be aware of the installation of the monitoring devices and their location. In particular, installation of surveillance cameras must be limited to working areas, bearing in mind the employees' right to integrity and intimacy. For instance, they cannot be located in bathrooms, rest areas or union premises. In summary, employers must comply with the information duty.

Regarding the above mentioned information duty, the most recent case law states that, as long as the worker is aware that the company has installed a video surveillance control system, the employer does not have to specify, beyond mere surveillance, the exact purpose assigned to those cameras. In other words, it does not have to be stated that the cameras can also be used, besides security reasons, for employment-related sanctioning purposes.

Nevertheless, from a data protection perspective the information requirement is more "rigid". The employer must: (i) place, in the video-surveyed areas, at least one informative distinctive/badge located in a sufficiently visible place, both in open and closed spaces, and, (ii) have at the disposal of the interested parties forms including the information provided in the Data Protection Act.

Notwithstanding the foregoing, as stated above, in accordance with recent case law, not displaying this informative badge does not necessarily entail the violation of a Fundamental Right. However, this infringement could entail administrative sanctions imposed on the company for not complying with the Data Protection Act provisions.

Moreover, another question discussed in relation to workers' monitoring is employees' consent. In this regard, according to the Data Protection Act, consent is not necessary because monitoring takes place within an employment relationship and such measures are necessary for the maintenance or compliance of the labour contract. This is an exception to the general rule.

In any case, the employer must use the least "aggressive" means to monitor the employees bearing in mind other circumstances such as whether:

- (i) the installation is carried out massively and indiscriminately;
- (ii) the monitoring systems are visible or hidden;

- (iii) the actual goal of the installation of the monitoring devices (assess whether it is suitable, proportional and necessary).

Regarding **computer monitoring**, such measures must be justified, necessary and balanced. Otherwise, they could infringe the employees' right to communications secrecy. In this sense, the employer must establish rules regarding the use of the IT devices and provide them to the employees before considering whether such use is appropriate from a disciplinary point of view.

Unless a Collective Bargaining states otherwise, although it is highly recommended, the employer is not obliged to communicate in writing to the employees the prohibition of the use of IT devices for private purposes. This prohibition can be evidenced by other means (for instance, by means of repeated verbal warnings or by including a message every time the employee turns the computer on). In any case, when there is an express prohibition which eliminates the employees' expectancy of privacy, it is licit to monitor the employees' computers to evidence that they did not obey such prohibition and sanction them accordingly.

Regarding the evidence obtained by accessing the employees' computers in court, the following points must be borne in mind:

- (i) there must be a specific, explicit and legitimate purpose;
- (ii) monitoring/access must be a proportional response to the threat;
- (iii) there must be minimum repercussions to the intimacy right of the employees;
- (iv) the employee and his / her representatives must be present when the employer accesses to the employee's email.

If these requirements are not met, there is a high risk that the evidence will be declared null and void by the Court.

Trends that can be identified

There are two relevant trends that can be easily identified regarding employees' monitoring:

1. Contradictory case law between the Spanish Supreme and Constitutional Courts and the ECtHR.

Spain is currently facing a situation of significant legal uncertainty regarding employees' IT monitoring:

- (a) Recent judgments of the Supreme Court and, especially, of the Constitutional Court seem to give greater freedom to corporate control and do not require compliance with the information duty stated under the Data Protection Act as long as the monitoring measures are suitable, proportional and necessary, and the employee is aware of them. As an example, in the case of the installation of surveillance cameras, the recent case law establishes that, with regard to the requirements established by the Data Protection Law (right of information), it is accepted that the company may fail to comply with this requirement, even if it is sanctioned for it. However, this does not affect the employees' rights as long as the measure is proportional to the objective.
- (b) On the other hand, the ECtHR (*Lopez Ribalda and Others v. Spain Applications 1874/13 and 8567/13*) was more protective of employees' rights. The ruling held that when installing covert cameras, the employer had not complied with the requirements of the legislation (Data Protection Act). In this sense, the employees should have been advised as to the personal data that would be processed on them. In addition, the ECtHR held that the employer's interest in protecting its property rights could be satisfied by other means such as informing employees of the installation of a system of video surveillance.

Bearing in mind the above, it is highly likely that the doctrine of the Supreme and Constitutional Courts will soon be modified in accordance with the recent ruling of the ECtHR. From a practical perspective, it is recommended that companies follow the doctrine of the ECtHR to avoid potential issues. In other words, despite Spanish case law, we suggest always complying with the information duty stated under the Data Protection Act; informing the employees about the installation of cameras and displaying the informative badge in a visible place.

2. Entry into force of the GDPR and the new Data Protection Act

The new GDPR (which will come into force in all EC member states on 25 May 2018), is the most relevant piece of EU legislation that will impact employee IT monitoring. In addition, the new Spanish Data Protection Act will come into force around this date.

It is highly likely that when the new Data Protection Act comes into force, companies will start informing employees, as allowed by said law, about the fact that surveillance cameras will also be used for labour monitoring purposes (and not just for security as is the case currently).

Bearing in mind the above, the entry into force of the GDPR and the new Data Protection Act entail that companies will have to update their employer's policy with regard to monitoring employees and Data Protection to avoid potential issues (fines, declaration of unfair/null dismissals etc.).

Existing case law

List of cases

1. *Coruñesa de Etiquetas, S.L. v. Mr. Imanol* Rec. 966/2006 (page 104)
2. *Ms. Elosia v. Global Sales Solutions Line, S.A.* 241/2012, Rec. 7304/2007 (page 105)
3. *Ms. Delia v. Bershka BSK España, S.A.* 39/2016, Rec. 7222/2013v (page 106)
4. *Dir Fitness, S.L. v. Mr. José Ramón* 96/2017, Rec. 554/2016 (page 107)
5. *Quorum Gestión Empresarial, S.L. v. Ms. Palmira* 226/2017, Rec. 55/2015 (page 108)

Case Name, Citation and Court	Coruñesa de Etiquetas, S.L. v. Mr. Imanol Rec. 966/2006 Supreme Court (Tribunal Supremo)
Date	26 September 2007
Subject	Employer's management power. Use of company's IT system.
Key facts	<ul style="list-style-type: none"> I, an employee of CE, worked at a keyless office where he had a computer, without an access code. An IT company was hired to check the failures of I's computer and viruses were detected for "<i>browsing through unsafe Internet pages</i>". In the presence of CE's director the folder of temporary files evidenced access to pornographic sites, which were stored on a USB device, and handed to a notary. The search was made with no presence of I, employees or representatives. The computer was removed from CE for repair and, once returned, the same operation was undertaken with the presence of employees' representatives. The Supreme Court dismissed the appeal file by CE.
Key points	<ul style="list-style-type: none"> The limits of the IT system monitoring are in relation to their impact on employees' dignity and privacy. The company must previously establish the rules of use and inform the employees that there will be monitoring and the means to implement it. Tolerance with personal use of the company's IT creates a confidentiality expectation but if the tool is used for private purposes against the company's prohibition and with knowledge of the control measures, no expectation of privacy is violated. It is not an obstacle to the protection of privacy that the computer does not have an access code or that the computer is located in a keyless office. CE could not collect the information in the temporary files, without prior warning about use and control of the computer, and use it for disciplinary purposes since it entailed a violation of I's right to privacy. CE's actions were not limited to the control and elimination of the virus since it was followed by the examination of the computer.

Case Name, Citation and Court	Ms. Elosia v. Global Sales Solutions Line, S.A. 241/2012, Rec. 7304/2007 Constitutional Court (Tribunal Constitucional)
Date	17 December 2012
Subject	Downloading an instant messaging program and sending personal messages
Key facts	<ul style="list-style-type: none"> • E worked for GSS. She was verbally warned on 27 December 2004 for downloading an instant messaging program without the authorisation or knowledge of the company. This was expressly prohibited. • The program was installed on a computer that was commonly used by workers without an access code. • E and another employee sent each other messages in which they criticized clients, partners and bosses and filed the communications in the computer. • Such communications were discovered by an employee who communicated it to the superiors. After an investigation, the employees were invited to a meeting and they were verbally warned, without any additional disciplinary action. • E appealed to the Constitutional Court in relation to infringement of the right to privacy and secrecy of communications. • The claim was based on the intimate nature of the messages and on the fact that the secrecy of the communications was violated when opening the files.
Key points	<ul style="list-style-type: none"> • The privacy right was not violated since the employees used a shared computer. • The employer's power of organisation allows him/her to regulate the IT use. • The Court considered two circumstances that arose in this case: (i) the computer was used by all the employees; (ii) GSS had expressly forbidden the workers to install programs in the computer. Thus, no expectation of confidentiality existed. • Such open communication systems as in this case are opposed to the concept of secrecy. The overall access process was respected when the finding was communicated to the management by an employee (casual finding) and this to the workers. • The Constitutional Court dismissed E's appeal.

Case Name, Citation and Court	Ms. Delia v. Bershka BSK España, S.A. 39/2016, Rec. 7222/2013 Constitutional Court (Tribunal Constitucional)
Date	3 March 2016
Subject	Employer's use of video surveillance at work
Key facts	<ul style="list-style-type: none"> • D was employed as a sales assistant in a shopping center for BSK and was terminated on 21 June 2012. BSK, after installing a new cash control system, detected that there were multiple irregularities in a cash register. BSK installed a video surveillance camera that controlled said register. • The camera was installed without telling the employees. However, information was displayed alerting people to its presence in a visible and distinctive place in the shop window. • D's dismissal letter stated that he had appropriated cash from the cash register, on different dates and on a regular basis.
Key points	<ul style="list-style-type: none"> • The Constitutional Court defined the scope of the information duty, fulfilled when the company placed the information displayed was within the conditions established by Spanish Data Protection. • The Court said that the duty to inform was fulfilled because the camera was located in the place where the work performance was developed, focusing directly on the cash register, and the informative badge was located in a visible place, in the shop window. D knew that BSK had installed a video surveillance control system, and BSK did not have to specify the exact purpose. • Even if BSK did not comply with the Data Protection Act (and it can even be sanctioned for that), that does not mean that the employees' rights are affected if the measure is proportionate. • The installation of cameras was a justified measure since there were suspicions that one of the employees was stealing; the installation was suitable for verification and to adopt disciplinary measures. The recording was a balanced measure as it was limited to the cash register area. • The Constitutional Court ruled that there was no Privacy Right infringement.

Case Name, Citation and Court	<i>Dir Fitness, S.L. v. Mr. José Ramón</i> 96/2017, Rec. 554/2016 Supreme Court (Tribunal Supremo)
Date	2 February 2017
Subject	Employer's use of video surveillance at work
Key facts	<ul style="list-style-type: none"> • JR, an employee, worked as a technical manager for DF, the company, and was terminated on 13 October 2014. DF had detected several irregularities in the gym where JR worked through the video surveillance cameras. Several employees complained about JR. • The cameras were installed at the entrance and at the public spaces of the gym. According to the Head of Security, the information displayed informing of such surveillance was in line with the requirements of the Spanish Data Protection Agency. • Surveillance authorisation does not include cameras for the use of monitoring working time or for disciplinary purposes. The workers were not warned directly of this surveillance. • JR was present when another employee was previously dismissed for similar reasons.
Key points	<ul style="list-style-type: none"> • Since JR knew (i) that another disciplinary termination, for the same reasons, was undertaken; and, (ii) that the cameras were installed, the Court stated that the cameras were intended to control irregularities. • JR's circumstances deserved special consideration (previous complaints posed by other employees). According to the Data Protection Act, DF did not need JR's express consent. Even if the company did not comply with the information duty as required by the Data Protection Act (and it can even be sanctioned for that), it did not mean that the employees' rights were affected if the measure was proportionate. • JR knew that the company had installed a surveillance system. The important issue was to determine if the data obtained was used for the purpose of controlling the employment relationship or for a different one; DF would need consent if the purpose was not directly related to the labour relationship. • The Supreme Court admitted the validity of the cameras as evidence.

Case Name, Citation and Court	Quorum Gestión Empresarial, S.L. v. Ms. Palmira 226/2017, Rec. 55/2015 Supreme Court (Tribunal Supremo)
Date	17 March 2017
Subject	Monitoring of employee's email sent to his lawyer which included litigation strategy.
Key facts	<p>P, an employee, was declared to be entitled to a working time reduction for legal guardianship reasons of a child aged under 12.</p> <p>QGE, the employer, appealed the judgment before the Supreme Court.</p> <p>The appeal was based on an email sent by P to her lawyer found by QGE.</p> <p>QGE argued that this email was found due to the fact that the employer had to continue with P's uncompleted job since she was on temporary disability leave.</p> <p>The email also included P's legal strategy. It was stated that she was asking for a new schedule which would probably not be accepted by QGE which would allow her to be terminated receiving a severance payment.</p> <p>QGE's appeal was dismissed by the Supreme Court.</p>
Key points	<ul style="list-style-type: none"> • The conditions of disposition and use of IT tools must be studied case by case to assess whether companies are entitled to monitor employees' IT tools. • The intensity of the measure (monitoring) and the rigidity of the rules (prohibiting the use of IT systems during working time) should be assessed. • The judgment mentions Barbulescu's case in which it was considered that monitoring the employee's "Yahoo Messenger", under the corresponding notice, was a lawful, reasonable, necessary and proportional measure. • However, the Supreme Court did not reach the same conclusion because QGE did not evidence: (i) the reasons for monitoring P's email, (ii) the existence of any previous instructions/policies regarding IT use, and, (iii) that it warned the employees about the company's right to monitor the IT system. Also, QGE had not detailed the procedure used to monitor P's computer (previous consent, presence of another worker, method) in order to guarantee P's intimacy right. • Furthermore, it was stated that even professional secrecy could be affected.

Summary of existing legislation

Introduction

In Spain, there are several pieces of legislation which regulate and place different restrictions on employee monitoring. The key acts of legislation are:

- Data Protection Act 1999 (and RD 1720/2007);
- Employment Act October 23, 2015;
- Collective Bargaining Agreements; and
- Spanish Constitution (Article 18).

A short summary of the restrictions on monitoring imposed by each is as follows.

Data Protection Act 1999 (and RD 1720/2007)

In Spain, the Data Protection Act constitutes the legal framework on privacy rights of individuals in connection with the processing of their personal data. The individual's right to control the processing of his/her personal data is considered a constitutional right to privacy. Therefore any processing of personal data must be informed to individuals and, as a general rule, subject to the prior consent of the data subject. The governmental agency authorized to monitor the creation, management, assignment and use of databases (whether automated or not) is the Spanish Data Protection Agency.

The personal data collected must be accurate, which may imply the implementation of mechanisms to confirm that the information collected (particularly from third parties other than the data subject) is truthful and updated. In this sense, the Data Protection Act requires the deletion of any personal data that is not accurate.

Personal data may only be used for legitimate business purposes and for so long as the personal data is required. Although LOPD does not define "*legitimate business purposes*", the Spanish Data Protection Agency has consistently admitted that, *inter alia*, the following uses would fall under this category:

- human resources management, including the use for payroll purposes, management of benefit plan and training programs;
- performance of legal and/or contractual obligations;
- education purposes;
- management of health and sanitary services, including the control and study of infectious diseases; and
- promotional purposes.

In all cases, the data controller must keep confidential any personal data collected and take the appropriate security measures to ensure that such information will not be accessed, used, copied, modified or cancelled by unauthorized users (see below our comments on security measures). The confidentiality obligation remains in force upon cancellation of the personal data.

Moreover, Article 5 of the Data Protection Act states the obligation of informing the employees in an express,

precise and unambiguous way of the following:

- existence of a file or treatment of personal data, the purpose of the collection of these and the recipients of the information;
- mandatory or optional nature of the responses to the questions asked;
- consequences of obtaining the data or the refusal to supply it;
- possibility of exercising rights of access, rectification, cancellation and opposition; and
- identity and address of the person responsible for the treatment or, where appropriate, of his/her representative.

In addition to this, *Instruction 1/2006 of November 8* issued by the Spanish Data Protection Agency about the treatment of personal data for surveillance purposes through cameras or video cameras states the following obligations must be borne in mind for those who have video surveillance systems to comply with the duty of information provided in said Article 5:

- placing, in the video-surveyed areas, at least one informative distinctive/badge located in a sufficiently visible place, both in open and closed spaces; and
- having at the disposal of the interested parties forms including the information provided in article 5.1 of the Data Protection Act.

In addition to this duty of information, articles 6.1 and 6.2 refer to another important issue - consent:

- the treatment of personal data will require the unambiguous consent of the affected party, unless the law provides otherwise; and
- consent will not be necessary when they refer to the parties to an employment contract and are necessary for its maintenance or compliance.

Ultimately, the Data Protection Act requires the employer to inform employees but consent is not required.

Upon infringement of any provision of the Data Protection Act, an investigation proceeding may be opened. The investigation proceeding must be filed by the data subjects or a legitimate third party (as it may be the consumer associations or other organization representing the interests of affected individuals), or ex officio by the Spanish Data Protection Agency.

Finally, the Data Protection Act provides 26 potential infringements. They are divided into three categories: minor, serious and very serious. These violations are subject to penalties ranging from EUR601 to EUR601,012.10, depending on the nature of the personal rights affected, the volume of data concerned, profits obtained, intent, continued nature of the infringement, etc..

In addition, civil courts may grant injunctive relief to individuals and award damage compensation.

Employment Act 23 October 2015

The Employment Act is the main code that governs ordinary labour relationships. It includes all main issues such as: types of contracts, modifications and terminations, workers representation, etc. The Employment Act also

regulates monitoring of employees. In this sense, for this report's purposes, the following Articles should be borne in mind:

- Article 4.2. Workers have the right to respect their privacy and due consideration to their dignity.
- Article 18. The employee, their locker and their personal effects may only be searched when it is necessary for the protection of business assets and those of other workers of the company. The search must be carried out in the workplace and during working hours. During the search, the dignity and privacy of the employee will have to be respected and employees will be assisted by the employees' legal representative or, in their absence from the workplace, by another worker of the company, whenever this is possible. (This Article does not really apply to IT monitoring but it is important to take it into consideration).
- Article 20.1. The employee must carry out the work agreed under the direction and follow the instructions provided by the employer.
- Article 20.3. The employer may adopt the measures they deem most appropriate for monitoring and controlling the working activity to verify compliance by the worker of their obligations and duties, keeping in its adoption and application due consideration to their dignity and taking into account, where appropriate, the real capacity of disabled employees.

In summary, bearing in mind the above, IT monitoring must always be undertaken bearing in mind employees' right to privacy and dignity.

Collective Bargaining Agreements

Collective Bargaining Agreements (**CBAs**) have been negotiated for specific industries across Spain (i.e. financial services). In this sense, each company will have to apply a specific CBA, which depends on the industry sector where the company develops its activities, being automatically bound by the rules established in it and, consequently, having to comply with the applicable agreement's rules on employment issues (i.e. working time, wages, temporary contracts, notice period, special rules for sickness situations, etc). Moreover, CBA's could be applicable within the national scope, a specific region or, even negotiated by the Company and employees' legal representatives at a company level.

CBAs may include infringements and sanctions related to monitoring of employees. For instance, the CBA for the Chemical Industry states under Article 59.11 that "*the use of the computer resources owned by the company (email, Intranet, Internet, etc.) for a purpose other than those related to the content of the work provision is a non-serious infringement with the exception of the provisions of the article 82.2. (use by the employees' representatives)*".

In this sense, CBAs can sanction misconduct regarding the use of IT but they can also state tolerance with regard to such use, prohibiting absolute restriction on the use of IT devices for private purposes.

Spanish Constitution (Article 18)

The Rights included in the Spanish Constitution result in restrictions imposed on the employers regarding workers' monitoring:

- Article 18.1: The right to honor, to personal and family privacy and to one's own image is guaranteed.
- Article 18.3: The secrecy of communications and, in particular, of postcards, telegraphs and telephones is

guaranteed, except for judicial decisions.

- Article 18.4: The law will limit the use of information technology to guarantee the honor and personal and family privacy of citizens and the full exercise of their rights.

When companies monitor the use of computer resources made available by the employer, the right to privacy and secrecy of communications must be respected. Regarding video surveillance, the right to privacy and data protection must be observed.

Future legislation which may have an impact on employee monitoring

New Data Protection Act (bill that will come into force, presumably, in May 2018)

The new Data Protection Act will probably come into force shortly after the GDPR. The new law, if approved as drafted, will allow employers to use security cameras at work centers to monitor employees' performance, beyond mere safety reasons. Thus, video surveillance will be used, among other purposes, to verify if employees comply with their work, if they respect the work schedule and to monitor their absences. The only requirement is that employees must be informed that the captured images can be used for these purposes.

Article 22.5 of this law states that employers may process data obtained through camera systems or video cameras to monitor employees, provided that these functions are exercised within their legal framework and with the inherent limits to it. Employers will have to inform workers about this measure.

In the event that the images have captured the flagrant commission of a criminal act, the absence of the information referred to in the previous section will not deprive the images of probative value, without prejudice to the responsibilities that may arise from said absence.

In this sense, the law further states that the duty of information foreseen in article 12 of GDPR will be understood as fulfilled by placing an informative device in a sufficiently visible place identifying, at least, the existence of the treatment, the identity of the person in charge and the possibility of exercising the rights provided for in articles 15 to 22 of GDPR.

Belgium

Commentary on existing case law

The existing case law set out below in this overview deals extensively with the balance between ensuring the protection of employees' fundamental rights, such as the right of privacy, and the employer's right to exercise authority over its employees and the related right of supervision. In these types of cases, it is not uncommon that infringements or offences committed by employees are uncovered during random controls by the employer. Accordingly, this case law must be read together with the evolution of the Belgian legal doctrine regarding illegally obtained evidence. This introductory section briefly sets out the evolution of this subject, first in case law, then in law.

In brief, the case law and the legal framework regarding illegally obtained evidence deal with the question as to what extent evidence of wrongdoing can be taken into account when it has been gathered in violation of applicable norms (e.g. the fundamental right of privacy of employees). Specific to employment law, examples include the fact that the employer uncovers in an unlawful way that employees have been misusing company assets, or have been carrying out personal tasks during working time.

In Belgium, the traditional view, as set out by the Court of Cassation in 1923, (*Hof van Cassatie / Cour de Cassation*), the highest civil court in Belgium, was that illegally obtained evidence must necessarily be taken out of the courts' consideration.

This view was left unaltered until 2003, when the Court of Cassation changed its jurisprudence with the so-called *Antigoon* case law. Since 2003 there are only three situations in which a court must rule out illegally obtained evidence:

- when the consequence of nullity is explicitly prescribed by law;
- when the illegality committed in obtaining the evidence has tainted the reliability of the evidence;
- when relying on the evidence would be in violation of the right to a fair trial.

In three later judgments, rendered in March and November 2004, the Court of Cassation further expanded on the scope of its *Antigoon* case law, stating that when assessing whether or not to rule out illegally obtained evidence, a court may also take into account whether or not the illegality has been committed intentionally, whether the degree of seriousness of the illegality is disproportionate to the value of the evidence, and whether the illegally obtained evidence proves only the material element of a crime, and not the intent of the perpetrator.

From an employment law perspective, this *Antigoon* case law was put into practice in the so-called *Manon* judgments, dealing with evidence of an employee of a chocolate store stealing from a cash register, obtained by a camera installed in violation of the applicable legal framework (for a summary of the applicable legal framework, we refer to section 1.C below, under the heading "*summary of existing legislation*"). The *Manon* judgments clarify that it is up to the court deciding on the case to verify whether the *Antigoon* principles set out above have been fulfilled. If so, the court must decide to rule out the evidence. If not, the court would be held to take the illegally obtained evidence into account.

Up to 2008, *Antigoon* case law was only applied in criminal cases. The Court of Cassation clarified however in the judgment of 10 March 2008 that the *Antigoon* case law is also applicable in civil matters. This case law has

been largely adopted by the lower courts in employment matters (i.e. in first instance: the labour tribunal (*arbeidsrechtsbank / tribunal du travail*), and in appeal: the labour court (*arbeidshof / cour du travail*)) (cf. infra).

Ultimately, the *Antigoon* case law was translated into a legal framework dealing with criminal law by way of the Law of 24 October 2013 (*Wet van 24 oktober 2013 tot wijziging van de Voorafgaande totel van het Wetboek van Strafvordering wat betreft nietigheden/ Loi du 24 octobre 2013 modifiant le titre préliminaire du Code de procédure pénale en ce qui concerne les nullités*). From a civil law perspective, which includes most employment law matters, the legal anchoring of these principles in matters of criminal law strengthens the uniformity by which these are applied in case law, although discussion sometimes remains.

Trends that can be identified

As set out above, there is a growing tendency to accept evidence in employment-related cases which has been gathered in violation of the applicable legal standards. Nevertheless, it should be noted that there are still a few absolute limits which may not be violated in this regard.

Concerning employment-related case law, another identifiable trend is that it is more and more accepted that private statements made on social media platforms can have an impact on an employment relationship and may lead to an employee's termination, even in cases where the statement concerned did not relate to the employer or the employment as such.

Existing case law

List of cases

1. *Court of Cassation – Second Manon judgment* (2 March 2005) (page 118)
2. *Labour Court of Brussels* (28 November 2006) (page 119)
3. *Labour Court of Liège* (11 January 2007) (page 120)
4. *Labour Court of Hasselt* (29 August 2007) (page 121)
5. *Court of Cassation* (10 March 2008) (page 122)
6. *Labour Court of Antwerp* (2 September 2008) (page 123)
7. *Labour Tribunal of Oudenaarde* (3 February 2009) (page 124)
8. *Labour Court of Brussels* (4 March 2010) (page 125)
9. *Labour Court of Ghent* (28 June 2010) (page 126)
10. *Labour Court of Liège* (20 September 2010) (page 127)
11. *Labour Tribunal of Namur* (10 January 2011) (page 128)
12. *Labour Court of Liège* (8 March 2011) (page 129)
13. *Labour Court of Brussels* (9 August 2011) (page 130)
14. *Labour Tribunal of Louvain* (17 November 2011) (page 131)
15. *Labour Court of Brussels* (3 September 2013) (page 132)
16. *Labour Court of Liège* (18 November 2011) (page 133)
17. *Labour Court of Brussels* (29 May 2013) (page 134)
18. *Labour Court of Ghent* (12 May 2014) (page 135)
19. *Labour Court of Brussels* (14 July 2014) (page 136)
20. *Labour Tribunal of Brussels* (12 September 2014) (page 137)
21. *Labour Court of Liège* (20 November 2014) (page 138)
22. *Labour Court of Liège* (17 November 2015) (page 139)
23. *Labour Court of Brussels* (19 September 2016) (page 140)

Court	Court of Cassation – Second <i>Manon</i> judgment
Date	2 March 2005
Subject	Taking into account illegally obtained evidence – camera surveillance
Key facts	<ul style="list-style-type: none"> An employee was suspected of stealing from the cash register of the chocolate store where she was employed. The employer installed a video camera to register these incidents, which indeed took place and were caught on video.
Key points	<ul style="list-style-type: none"> The Court of Cassation ruled out the evidence in a first judgment of 9 June 2004. In a second judgment, dated 2 March 2005, the Court of Cassation allowed the court in question to decide whether the evidence could be taken into account, based on the <i>Antigoon</i> case law. Accordingly, the court was to determine whether the evidence was tainted by any of the following situations; <ul style="list-style-type: none"> when the consequence of nullity is explicitly prescribed by law; when the illegality committed in obtaining the evidence has tainted the reliability of the evidence; and when relying on the evidence would be in violation of the right to a fair trial.

Court	Labour Court of Brussels
Date	28 November 2006
Subject	Privacy of employees – monitoring of hard disk or other hardware
Key facts	<ul style="list-style-type: none"> Following a routine supervision, it was uncovered that an employee actively participated on an escort service website. This was uncovered after an IT specialist had pointed to the exceptionally large volume of the “<i>my documents</i>” and “<i>my files</i>” folders on that employee’s hard drive.
Key points	<ul style="list-style-type: none"> The court found that the documents could lawfully be accessed by the employer in cases where such information is discovered by accident, and where it could be assumed that the files might be of a professional nature.

Court	Labour Court of Liège
Date	11 January 2007
Subject	Privacy of employees – monitoring hard disk or other hardware
Key facts	<ul style="list-style-type: none"> An employee stored personal information on the hard disk of an employer's computer.
Key points	<ul style="list-style-type: none"> The court found that, unless it concerns personal correspondence, access by an employer to personal information stored on an employer's computer is lawful. By storing such personal information on that hard disk, the employee knowingly takes a risk that this information can be accessed by anyone who uses that particular computer.

Court	Labour Court of Hasselt
Date	29 August 2007
Subject	Collective bargaining agreement n° 81 – private nature of emails and telecommunications of employees
Key facts	<ul style="list-style-type: none"> An employee accessed a former firewall which was no longer in use without his employer's consent in order to hide certain online activities, such as sending personal emails during working time.
Key points	<ul style="list-style-type: none"> The Court ruled that, as the firewall was no longer in use, these telecommunications were not covered by Collective bargaining agreement n° 81. It was found that Collective bargaining agreement n° 81 applied only to telecommunications sent by way of software provided by the employer. As such, the employee's telecommunications were not protected by the provisions of collective bargaining agreement n° 81.

Court	Court of Cassation
Date	10 March 2008
Subject	Taking into account illegally obtained evidence in employment cases
Key facts	<ul style="list-style-type: none"> Police authorities had sent a fax message to the labour inspection, in which they indicated that a person who was registered as being unemployed was in fact working illegally in his brother's store. In the ensuing procedure, the defendant argued that the police unlawfully disclosed information from an ongoing criminal investigation to the social inspection without approval of the public prosecutor, as a result of which the secrecy of the criminal investigation was violated.
Key points	<ul style="list-style-type: none"> The Court of Cassation applied, for the first time, the <i>Antigoon</i> and <i>Manon</i> case law to a civil dispute, stating that the same principles applied to the question whether evidence in civil matters should be taken into account. Accordingly, the <i>Antigoon</i> principles, defining the exact circumstances when evidence must be ruled out of the consideration of a court, (i.e. when the consequence of nullity is explicitly prescribed by law, when the illegality committed in obtaining the evidence has tainted the reliability of the evidence, or when relying on the evidence would be in violation of the right to a fair trial,) was also to be applied in full in civil and employment matters, and not only in criminal trials.

Court	Labour Court of Antwerp
Date	2 September 2008
Subject	Taking into account illegally obtained evidence in civil cases – private use of internet and email – application of <i>Manon</i> case law by lower employment courts
Key facts	<ul style="list-style-type: none"> An employer conducted a routine check and gathered evidence from work computers regarding the use of internet and email for personal reasons. An employee argued that this routine check violated the right of secrecy of telecommunications.
Key points	<ul style="list-style-type: none"> The court found that the illegality committed in obtaining the evidence had to be assessed in light of the <i>Antigoon</i> principles (i.e. that evidence must only be ruled out of a court's consideration when the consequence of nullity is explicitly prescribed by law, when the illegality committed in obtaining the evidence has tainted the reliability of the evidence, or when relying on the evidence would be in violation of the right to a fair trial). The court ruled that the illegality committed was of a minor character, meaning that its reliability was not affected and that it did not affect the right to a fair trial. Accordingly, the evidence could be taken into account.

Court	Labour Tribunal of Oudenaarde
Date	3 February 2009
Subject	Collective bargaining agreement n° 81 – legality principle limiting right of privacy
Key facts	<ul style="list-style-type: none"> • A dispute between an employee and employer arose regarding the use of internet and email on company computers.
Key points	<ul style="list-style-type: none"> • According to the tribunal, the employer should have instructions in place, in whatever form, such as a policy, to be authorised to supervise the use of internet and email of its employees.

Court	Labour Court of Brussels
Date	4 March 2010
Subject	Social media statements and termination
Key facts	<ul style="list-style-type: none"> A supermarket employee made negative statements on the Facebook page of the supermarket store that employed him. The negative statements related to the company he worked for, as well as his direct manager. The employee in question was a trade union delegate, meaning that he enjoyed additional protection against termination. The Facebook webpage in question was only visible to the employee's co-workers of a similar hierarchical level.
Key points	<ul style="list-style-type: none"> The court addressed in depth the question of publicity and stated that the employee was not aware that his statements could be regarded as being public in nature. The court found that the employee had erred by violating his duty of loyalty towards his employer, but that the facts as such did not amount to gross misconduct, so that the immediate termination of the employment agreement was not justified.

Court	Labour Court of Ghent
Date	28 June 2010
Subject	Taking into account illegally obtained evidence in civil cases – private use of internet and email – application of <i>Manon</i> case law by lower employment courts
Key facts	<ul style="list-style-type: none"> An employer systematically monitored the internet history of a particular employee.
Key points	<ul style="list-style-type: none"> The court found that this monitoring was done in violation of applicable norms. However, the reliability of the evidence was not affected by this illegality, and the right to a fair trial was equally not affected. Accordingly, the evidence was allowed to be taken into consideration.

Court	Labour Court of Liège
Date	20 September 2010
Subject	Privacy of employees – monitoring of hard disk or other hardware
Key facts	<ul style="list-style-type: none"> An employee made a CD-ROM which had been acquired by the employer.
Key points	<ul style="list-style-type: none"> The court found that, if such a disk contained personal information, the right of privacy had to be respected and the employer could not access this information, even if the computer in question belonged to the employer. However, if the disk contained information relating to the employer, which was accessible without a password and it could not be reasonably deducted that the information was of a personal nature, this information could lawfully be accessed by the employer.

Court	Labour Tribunal of Namur
Date	10 January 2011
Subject	Social media statements and termination
Key facts	<ul style="list-style-type: none"> An employee who worked in the kitchen of a retirement home made racist comments on Facebook about one of her co-workers, a woman of Albanian descent. The co-worker in question was not the employee's superior.
Key points	<ul style="list-style-type: none"> The issues of the case concerned the right to privacy of the particular employee. The tribunal condemned the statements made by the employee, but stated that they must be regarded in their proper context. The tribunal decided that an official warning would have been warranted, and that an immediate termination for gross misconduct was disproportionate in the case at hand.

Court	Labour Court of Liège
Date	8 March 2011
Subject	Taking into account illegally obtained evidence in civil cases – use of camera surveillance – application of <i>Manon</i> case law by lower employment courts
Key facts	<ul style="list-style-type: none"> A casino employee was suspected of committing fraud by conspiring with a casino player. The employer illegally installed a camera to prove his suspicions.
Key points	<ul style="list-style-type: none"> The court allowed the evidence by referring to the Court of Cassation's <i>Manon</i> case law. As such, it became clear that lower employment courts were accepting the application of the <i>Antigoon</i> principles in civil cases, thus following the Court of Cassation's <i>Manon</i> approach.

Court	Labour Court of Brussels
Date	9 August 2011
Subject	Taking into account illegally obtained evidence in civil cases – private use of internet and email – application of <i>Manon</i> case law by lower employment courts
Key facts	<ul style="list-style-type: none"> An employer monitored the internet history of a particular employee. It was found that the employee had spent a substantial amount of working time on non-work related matters, and more particularly relating to a business operated by his spouse. The court had to answer the question as to whether the evidence had been committed illegally and the consequences thereof on whether the court could rely on the evidence.
Key points	<ul style="list-style-type: none"> Because the employee had not been informed of the monitoring, the evidence was gathered illegally. However, the question of whether it would have to be taken into account was to be adjudicated in line with the Antigoon principles, (i.e. that evidence must only be ruled out of a court's consideration when the consequence of nullity is explicitly prescribed by law, when the illegality committed in obtaining the evidence has tainted the reliability of the evidence, or when relying on the evidence would be in violation of the right to a fair trial). However, the court ultimately refused to take the evidence into account, since this would lead to a situation where Collective bargaining agreement n° 81 would no longer be applied, and the right to privacy of employees would systematically be infringed.

Court	Labour Tribunal of Louvain
Date	17 November 2011
Subject	Social media statements and termination
Key facts	<ul style="list-style-type: none"> An employee, who fulfilled the task of a business development manager at a publicly listed company, was discovered to have made negative comments on several news items relating to his employer on his Facebook page. In these comments, the employee in question falsely presented himself as a commercial manager for Asia. The employer terminated the employment agreement immediately for serious cause.
Key points	<ul style="list-style-type: none"> The tribunal did not accept the employee's arguments as regards his privacy, due to the public nature of the comments in question. Nevertheless, the tribunal did attach some importance to the right of free speech of the employee. However, this was regarded as subordinate to the public nature of the comments, which was assessed separately from the issue of whether the comments were appropriate. The tribunal thus accepted the termination in light of the violation of the duty of loyalty of the employee.

Court	Labour Court of Brussels
Date	3 September 2013 (appeal judgement of previous case)
Subject	Social media statements and termination
Key facts	<ul style="list-style-type: none"> This is the appeal judgment against the judgment of the Labour Tribunal of Louvain of (17 November 2011 – see above).
Key points	<ul style="list-style-type: none"> The court made the distinction between the personal and the public area of someone's Facebook page, and stated that a person may have different reasonable expectations of privacy, depending on the area in which comments or statements are posted. In this case, the employee had posted comments on the public area of his Facebook page, so that he should have known that these would be publically accessible. Accordingly, the decision of the tribunal was confirmed.

Court	Labour Court of Liège
Date	18 November 2011
Subject	Collective bargaining agreement n° 81 – private nature of emails and telecommunications of employees
Key facts	<ul style="list-style-type: none"> An employee sent an email from his personal email address to a co-worker's professional email address. The co-worker informed the employer of the content of this email.
Key points	<ul style="list-style-type: none"> The court ruled that Collective bargaining agreement n° 81 does not apply to such emails, as they were sent from a personal account.

Court	Labour Court of Brussels
Date	29 May 2013
Subject	Social media statements and termination
Key facts	<ul style="list-style-type: none"> Several security agents had recorded a video of one security agent who, during working time, had taken off his shirt and was, at his request, beaten by his colleagues. The video was posted on Facebook and the employee was terminated immediately for serious cause. The employer cited reasons of its reputation being tarnished by the video and the apparent unprofessional behaviour of the employee in question.
Key points	<ul style="list-style-type: none"> The court found that the employee in question was not aware of the fact that the video would be made public. Because the acts took place in an area inaccessible to the general public, the video was made in a private setting. Accordingly, the court dismissed the termination for serious cause.

Court	Labour Court of Ghent
Date	12 May 2014
Subject	Excessive private use of company mobile phone – privacy of employee and supervision thereof – reasonable expectation of privacy
Key facts	<ul style="list-style-type: none"> An employee made a substantial amount of expensive phone calls during his working time. The employer paid the mobile phone subscription, but only allowed partial private use. The employer had claimed damages due the excessive amounts of phone calls made during working time.
Key points	<ul style="list-style-type: none"> The court found that an employer was entitled to supervise a cell phone subscription for which it is paying, even if part thereof allows for private use. The fact that the employer paid the subscription meant that the employee could not reasonably expect the content of his monthly invoice to be of private nature.

Court	Labour Court of Brussels
Date	14 July 2014
Subject	Social media statements and termination
Key facts	<ul style="list-style-type: none"> An employee responsible for the communication strategy of a multinational automobile manufacturer posted negative statements about her employer via Twitter. The employer dismissed her for serious cause.
Key points	<ul style="list-style-type: none"> The court confirmed that each employee is entitled to the right of free speech, but that this must be reconciled with the duty of loyalty towards an employer. Accordingly, and especially in view of the employee's function, the dismissal for serious cause was confirmed.

Court	Labour Tribunal of Brussels
Date	12 September 2014
Subject	Social media statements and termination
Key facts	<ul style="list-style-type: none"> An employee in a managing function had made negative statements about her job and the hierarchical structure of her employer on Facebook. The statements were made on the private area of her Facebook page, but were visible to all of her Facebook friends, which included colleagues and clients. The employer terminated the employment agreement for serious cause.
Key points	<ul style="list-style-type: none"> The tribunal confirmed the termination for serious cause because of the level of publicity that the post in question had. The tribunal stated that employees who choose to share information on a social networking site must be fully aware that such information is generally accessible to all internet users, and that this may result in substantial damages for the employer. Even if comments are only visible to a user's personal network, an employee may not always be able to hide behind the right to privacy. The limit placed by the tribunal appears to be the point when a comment or statement becomes insulting.

Court	Labour Court of Liège
Date	20 November 2014
Subject	Taking into account illegally obtained evidence in civil cases – secretly recording of communication – application of <i>Manon</i> case law by lower employment courts
Key facts	<ul style="list-style-type: none"> An employee secretly recorded a conversation with his employer regarding the payment of a variable wage. The question put before the court was whether the evidence could be taken into account, given the fact that it was obtained illegally, as the employee had recorded the conversation without obtaining the consent of his employer.
Key points	<ul style="list-style-type: none"> The court found that the evidence could only be ruled out if it was determined that one of the <i>Antigoon</i> principles had been violated. As the conversation was recorded in the workplace, and it only concerned the payment of the variable wage, and no other elements, it was taken into account by the court.

Court	Labour Court of Liège
Date	17 November 2015
Subject	Privacy of employees – monitoring of hard disk or other hardware
Key facts	<ul style="list-style-type: none"> An employer had requested to access and print out professional files stored on an employee's computer which pointed to illegal competition by that employee. This was done in the presence of a bailiff. The labour court had to answer the question as to whether this was an unlawful infringement into the employee's privacy.
Key points	<ul style="list-style-type: none"> The court found that this was lawful as the files did not in any way indicate that they would be of a personal nature and they were stored on a computer provided by the employer.

Court	Labour Court of Brussels
Date	19 September 2016
Subject	Taking into account illegally obtained evidence in civil cases – usage of internet and email – application of <i>Manon</i> case law by lower employment courts
Key facts	<ul style="list-style-type: none"> An employer accidentally listened to a recorded message which affected his interests.
Key points	<ul style="list-style-type: none"> The court found that, while the access to the information had indeed been involuntary, the evidence could nevertheless not be taken into account, as the employee had not consented thereto. Moreover, it was alleged that the employer had, after accidentally hearing the message in question, deliberately accessed other recorded messages. The actions of the employer were found to be a disproportionate infringement of the right to privacy of the employee.

Summary of existing legislation

From a legal perspective, the monitoring of employees specifically impacts the rights and obligations of the parties to an employment agreement on two key points. On the one hand, a balance must be struck between the employer's right to exercise its legally protected right of supervision and the employee's right of privacy. On the other hand, the obligation of loyalty to the employer in some cases conflict with an employee's right to free speech. The rapid advancement of technological communication and social media platforms have not surprisingly led to a plethora of case law, and legislators have in some cases not been able to keep up with this changing environment. In this section, we discuss the legal frameworks applicable to the core issues of privacy and free speech in the context of an employment relationship.

1. The employer right to supervise vs. the employee's right of privacy

The right of privacy is protected by various international human rights treaties, as well as by article 22 of the Belgian constitution. Because it is a fundamental right, any limit to the right of privacy must correspond to three key principles, required to limit any fundamental right. First, any limit must strive to contribute to a *legitimate objective*. Specific to the issue of privacy in the workplace, typical objectives include the protection of the employer's interests, the organization of efficient working relationships, etc. The employer has the right to exercise authority over his/her employees, which implies the right of supervision and control. Second, any limitation to the right of privacy must be *proportional* to the objective which is pursued. Third, the principle of *legality* should be respected. Specifically, this means that the limitation should be provided by law or one or more provisions that are sufficiently accessible and precise (not necessarily formal laws, but work rules, policies, etc.). The employee should have clarity on the applicable rules, limiting his right of privacy and therefore this principle is focused on transparency. This principle also allows the employer to take action in violation of the fundamental right of privacy.

The limitations to employees' privacy are generally carried out with regard to specific issues. The most controversial issues in this regard are discussed below together with their applicable legal framework.

1A. Protection of personal data

Employers are, as all other persons and entities, bound by the provisions of the Belgian Privacy Law of 8 December 1992 (*Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens / Loi de 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, the **Privacy Law**). This legal source must be interpreted in line with official advice issued by the Belgian Data Privacy Commission (*Commissie voor de bescherming van de persoonlijke levenssfeer / Commission de la protection de la vie privée*), which, although (currently) not having any official legal force, are regarded as authoritative interpretations of the legal framework surrounding data privacy.

In application of the GDPR (General Data Privacy Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, the **GDPR**), the Privacy law will thoroughly be reformed or replaced by May 2018. Most provisions will be replaced by the corresponding provisions of the GDPR. Also the composition and operational activities of the Belgian Data Privacy Commission is reformed. The Belgian Data Privacy Commission will become "Gegevensbeschermingsautoriteit" or Data Protection Authority as from 25 May 2018 and will have the authority to investigate and sanction.

The processing of personal data will be limited thoroughly. If the processing of certain personal data (in the employment relationship) is not legitimated by a legal or legitimate interest, explicit and informed permission of the employee will be necessary. Further the processing of "sensitive data" (such as data on race, religion, etc.) is prohibited. In general employees, will have more rights under the GDPR regarding the processing of their personal data: they will have the right to access (and receive a copy), change and delete their personal data.

1B. Secrecy of telecommunication

The right of privacy and to not have one's personal telecommunications supervised is specifically protected by the Law of 13 June 2005 regarding electronic communications (*Wet van 13 juni 2005 betreffende de elektronische communicatie / Loi de 13 juin 2005 relative aux communications électroniques*, the **Electronic Communications Law**), as well as articles 259bis and 314bis of the Belgian Penal Code.

Pursuant to article 124 of the Electronic Communications Law, no one may purposefully monitor another person's electronic communications. Pursuant to article 314bis of the Belgian Penal Code, it is even a crime to monitor another person's electronic communications (without his/her permission).

The Electronic Communications law, however, provides exceptions to the rule included in article 124. The monitoring of electronic communication is allowed in the following situations:

- when such actions are allowed or prescribed by law;
- with the permission of all involved persons in the communication;
- as proof of commercial transactions;
- when the only purpose is the control of the quality of service in call centers.

In an employment context, the first and second exception is relevant. With regard to the first exception, reference can be made to article 17 of the Employment Contract Act of 3 July 1978 (**Employment Contract Act**) which provides that the employee should work in conformity with the instructions of the employer with regard to the execution of his/her employment contract. The (former) Privacy Commission took the view that this article 17 of the Employment Contract Act , which sets out the specific obligations of any employee, provides for such a legal basis allowing monitoring of electronic communications provided that this is "foreseeable" for the employee (e.g. by a policy). On the other hand, the parliamentary preparatory works of the Electronic Communications Law and article 314bis of the Belgian Penal Code deal extensively with the issue of what constitutes consent of an employee to have his or her electronic communications monitored. In this regard, it should be noted that several legal scholars have defended the view that an employee implicitly consents to the monitoring of electronic communications simply by taking note of a company-wide policy which states so.

It should also be noted that for access to internet websites and email specifically, the collective bargaining agreement n° 81 of 26 April 2002 applies. This collective bargaining agreement, which is a legal source of employment law, was in fact adopted specifically because of the legal uncertainty relating to the monitoring of employees' internet history and email exchanges. As such, the Collective bargaining agreement n° 81 clarifies the framework in which and the conditions under which employees' communications can be monitored.

Pursuant to Collective bargaining agreement n° 81, the monitoring of electronic communications is only allowed when one or more of the objectives set out below are pursued:

1. preventing unlawful or defamatory events from taking place (e.g. hacking of computers, consultation of porn or pedophile websites, etc.);
2. protection of economic, trade-related and financial interests of the company (e.g. depleting advertising, violation of business secrets, etc.);
3. safety and/or decent technical functioning of the IT networking systems (e.g. downloading of heavy files, distribution of malware, etc.);
4. ensuring compliance with the IT related principles and rules applicable within the company.

Moreover, an employer must ensure that the monitoring is limited to the minimum extent required to achieve the objectives set out above. Further the possibility of control should be included in a policy and communicated to the employees.

1C. Cameras in the workplace

The issue of installing camera surveillance equipment in the workplace is addressed by Collective bargaining agreement n° 68 of 16 June 1998, which was declared generally binding by way of a royal decree of 20 September 1998. It should be noted that this Collective bargaining agreement must be read alongside the Privacy Law, which also deals with the issue of camera monitoring of employees.

Pursuant to Collective bargaining agreement n° 68, camera surveillance is only allowed if it is installed in order to achieve one or more of the objectives set out below:

1. safety and health;
2. protection of a company's assets and/or stock;
3. supervision of the production process concerning the machinery;
4. supervision of the production process concerning the employees;
5. supervision of the employee's working performance.

It should be noted that camera surveillance aimed at achieving objectives numbers 1 – 3 may be permanent, but that camera surveillance aimed at achieving objectives numbers 4 and 5 must be of a temporary nature.

Moreover, the surveillance must be limited to the minimum extent required to ensure that the objectives set out above are achieved. Further, the employees and the Privacy Commission should be properly informed by the employer on this camera surveillance, the objectives thereof, whether or not the data are being saved, the amount and localization of the cameras and the active periods of the cameras. Secretly installed cameras are therefore not in line with Collective bargaining agreement n°68.

1D. Checking an employee's hard disk or other hardware

Regarding the monitoring of an employee's hard disk or other hardware, specific case-law exists which must be taken into account. For a summary of these cases, we refer to our overview of applicable case-law.

2. Employees' right of free speech and employer's reputation

As is the right to privacy, the right to free speech is fundamental, but not absolute. It can therefore be limited in

line with the principles set out above, which are finality (legitimacy of objectives pursued), proportionality and legality. From an employment law perspective, the inherent tension between the right to free speech and the relationship of authority which is one of the essential elements of any employment agreement most often translates into disputes surrounding (i) issues of recruitment based on information about the candidate found online, and (ii) the private nature and consequences of insulting, defamatory or racist statements made by an employee on social media platforms in their capacity as private persons.

When considering these issues, it is important to note that in case law, the employment courts and the Court of Cassation attach a great deal of importance to the criterion of a reasonable expectation of privacy. More specifically, it is stated that when assessing private communications, the courts must take into account the extent to which the person involved could reasonably assume that his or her statements, which include online information, would remain private at the time when they were made or the information was posted.

2A. Recruitment and online background checks

Collective bargaining agreement n° 38 of 6 December 1983 applies specifically to the issue of recruitment. Pursuant to article 11 of this collective bargaining agreement, the personal life and privacy of the candidate must be taken into account during the recruitment procedure. This means that any questions or inquiries regarding a candidate's or applicant's personal life must be reasonably related to the nature of the position that that person is applying for. This is referred to as the principle of relevance. In more recent times, this principle of relevance has moreover been interpreted as applying in full to inquiries of social media history and inquiries of potential candidates.

In addition to the provisions of Collective bargaining agreement n° 38, the issue of taking into account personal information during recruitment processes is also governed by the provisions of the Privacy Law. Pursuant to article 1, § 2 of the Privacy Law, the processing of personal data includes accessing, consulting or requesting personal information, so that simply gathering and saving personal information about a potential candidate or applicant from online sources falls under the scope of the Privacy Law. For the sake of completeness, it should be noted that this viewpoint was challenged by some legal doctrine, stating that mere consulting of online information, such as a routine screening of applicants would not be subject to the provisions of the Privacy Law. Nevertheless, as the GDPR will soon enter into force, it should be noted that it is generally accepted that such screenings would indeed fall under the scope of application of the GDPR insofar as the result of these screenings are 'processed'.

Pursuant to the application of GDPR, an employer who decides to screen a potential candidate or applicant must comply with the provisions of this legal framework. This means that such screening must be done in compliance with the general principles set out by the GDPR, and that specific safeguards apply to the processing of sensitive personal information. Equally important is the obligation to inform a potential candidate or applicant that such personal information has been processed, as under the GDPR he/she has the right to access, change or delete this information.

Finally, it should be pointed out that in addition to the specific safeguards surrounding the processing of sensitive personal information, which includes information as regards someone's ethnicity or racial background, which can only be processed in a limited amount of cases, an employer must also comply with the legal framework concerning antidiscrimination. Pursuant to the aforementioned Collective bargaining agreement n° 38, which binds all employers in Belgium, the job applicant's privacy rights must be respected during the recruitment, selection and hiring process, and inquiries into the job applicant's private life are only justified if they are relevant

to the nature and conditions of the job. As such, the question of permissibility of background checks must be determined on a case by case basis.

2B. Private statements on social media platforms within the context of an employment relationship

As soon as someone enters into an employment agreement as an employee, he or she becomes bound by a duty of loyalty towards that employer, who is entitled to exercise authority over that employee. These duties are implied in article 16 and 17 of the Employment Contract Act.

In principle, an employer has no authority over the actions and activities pursued by his or her employee during that employee's personal time. Nevertheless, the principle of loyalty towards an employer means that there are some limits to what an employee can do in his or her personal time. For example, an employee may not, whether during working time or not, make public confidential business information. In the same sense, an employee must refrain, even outside of working times, from conducting any action that would harm his or her employer. It is generally accepted that certain activities by an employee conducted during that employee's personal time can negatively impact the interests of an employer, and can therefore come under the scope of the employment relationship and the duties enshrined in the Employment Contract Act (duty of loyalty towards the employer).

In light of the principles set out above, we refer to the overview of case law, in which several cases have been included dealing with termination of an employment agreement due to statements made online or on social media platforms by an employee during his or her personal time, but which negatively affected an employer's reputation or that employee's working relationship with colleagues or the employer. From these cases, it becomes clear that such statements may ultimately lead to an employee's termination, if it can be determined that they negatively and sufficiently impact an employer's reputation or other legitimate interests.

3. Whistleblowing

Whistleblowing is permissible under Belgian law insofar as the employer has a *legitimate interest* to bring serious infringements to light. Whistleblowing, however, implies sometimes the processing of sensitive data which needs the explicit permission of the involved persons. The Privacy Commission (as from 25 May 2018: Data Protection Authority) however accepts the processing of this data if the employees are well informed (e.g. through a whistleblowing policy. Such policy should be drafted in accordance with the following guidelines:

- finality (which notifications can be made);
- procedure (which procedure should be followed and anonymity of the reporter should be reported);
- proportionality (it is not possible to address this issue in another way);
- transparency (the employees should be informed on the system);
- safety (anonymity should be guaranteed);
- rights of the reporter and the complainant (the complainant should be informed of the complaint and his rights in this regard asap, the reporter should be informed on the outcome of his complaint).

Moreover, a whistleblower policy must be notified to the Privacy Commission (at least until the entry into force of the GDPR), as it concerns a data processing system. It is likely that this will be treated differently when the GDPR entries into force.

Future legislation which may have an impact on employee monitoring

On 25 May 2018, the GDPR will enter into force. Notwithstanding the fact that this Regulation will have direct effect in the Belgian legal order, several aspects of this new legislation will still require implementing measures in Belgium. At this point, it is unclear which specific measures will be adopted in this light. Further the European Commission is planning to adopt a new Regulation regarding privacy and telecommunication by 25 May 2018, which will probably change the rules currently included in the Belgian Law on electronic communication. Other than these measures, we have not directly come across any legislation which can be expected in the near future dealing with the issues addressed in this overview.

North America

Executive summary

In comparison to the EU, the **US** lacks a comprehensive federal privacy regime. Indeed, this was a primary factor in the demise of the EU-FTC Safe Harbor data transfer vehicle. In fact, although the Fourth Amendment to the US Constitution contains protections against unlawful searches and seizures, this Constitutional prohibition only restricts governmental action, not the action of non-governmental, private parties.

For the most part, the US has been more concerned about the destruction of relevant information than the "right to be forgotten." For that reason, most US record retention policies tend to focus on how long documents must be retained to meet statutory retention and litigation hold requirements to avoid spoliation of evidence concerns than when they must be deleted. There are, however, some pockets of legislation where the federal government has adopted nation-wide privacy laws applicable to employers in the private sector: the Health Insurance Portability and Accountability Act (**HIPAA**) governing health information; the Genetic Information Nondiscrimination Act (**GINA**) prohibiting health insurers and employers from discriminating on the basis of genetic information; the Family Medical Leave Act (**FMLA**) and American With Disability Act (**ADA**) addressing medical leave and/or accommodation for employees or family members; the Fair Credit Reporting Act governing collection of credit and background information for among other purposes, employment; the Computer Fraud and Abuse Act governing unauthorized access or exceeding authorized access to computers with intent, for among other reasons, to defraud or cause damage to a computer used in or affecting interstate or foreign commerce or communications, including cellphones; and the Electronic Communications Privacy Act (**ECPA**), making the unauthorized interception of wire, oral or electronic communications ("wiretapping or electronic eavesdropping") a crime; and the Stored Communications Act, which amended the ECPA, and governs access to stored electronic communications.

The National Labor Relations Board (**NLRB**) has taken the position that employee's negative comments about the workplace may be protected "*concerted activity*" speech, including when it is stated on social media. This employee protection has extended beyond that which has been permitted in most other countries around the world.

Most of the data privacy protections, to the extent they exist, emanate from the states, and in some cases cities, rather than US national government. Unlike the US Constitution, California has a Constitutional Right of Privacy in its First Amendment which extends to the private sector. Even with this state-wide constitutional protection, however, California case law has not extended privacy protections as far as that offered in the EU. For the most part, employers are free to monitor company equipment (company servers, laptops, company issued phones) with or without notice or consent of employees, although it is considered best practice to affirmatively negate any expectation of privacy by so advising employees that anything on company equipment may be monitored and reviewed at any time. There are, however, some exceptions such as if the employer knows that it is reviewing privileged attorney client communications. BYOD law is just developing but for the most part an employee's ability to conduct business on their personal phone is a privilege rather than a right. Therefore it too can be monitored but again, it is best practice to affirmatively negate an expectation of privacy as a quid pro quo for permitted migration of company information onto BYOD's. Social media policies, largely driven from the federal National Labor Relations Board has extended very expansive protections to non-supervisory employees to condemn their supervisors and workplace on social media sites as protected "*concerted activity*". New York and federal law permit recording of conversations provided at least one of the parties consent to the recording, whereas California law requires that all parties must consent to recording if there is a reasonable expectation of confidentiality.

All US states (except for Alabama and South Dakota) as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have adopted data security breach notification laws. Many states, including California, New York and Massachusetts have additional and more restrictive laws governing social security number collection, credit and background checks, additional health information protections, and additional recording and surveillance restrictions.

In addition, 30 states and 150 cities in the US have enacted "Check the Box" or "Second Chance" legislation which prohibits inquiry into a person's criminal convictions, at least prior to an offer of employment being extended. Because it is estimated that as many as one-third of Americans have some criminal record, these laws were enacted to give applicants a "second chance" rather than necessarily to protect their privacy, but they need to be identified and complied with to avoid liability. California, Massachusetts and New York (as well as a number of other states as well as cities in these and other states) have also enacted legislation prohibiting an employer from inquiring about an applicant's prior compensation, at least prior to an employment offer being extended. The rationale for these prior compensation inquiry laws, however, is also not rooted in privacy concerns, but rather out of concern that such questions perpetuate prior wage discrimination which has led to gender (and racial) wage disparities.

The legal position in **Canada** is similarly complicated. Since employment law is a provincial jurisdiction, each of the 10 provinces and the three territories have the authority to pass their own employment and privacy legislation. In addition, federal law governs federally-regulated employers, including airlines, telecommunication companies, interprovincial and international railways, interprovincial and international trucking, and banks.

There is detailed federal legislation in relation to the protection of personal information in trade and commercial activities – the Personal Information Protection and Electronic Documents Act (with the exception of Quebec, Alberta and British Columbia who have substantially similar legislation) which applies to federally regulated employers (as well as non federally regulated employers to the extent explained in the Canada chapter).

This incorporates 10 principles in relation to the collection, use, retention, disclosure and access to personal information as follows: accountability, identifying purposes, consent, limiting collection, limiting use disclosure and retention, accuracy, safeguards, openness, individual access and challenging compliance.

Note also legal restrictions are imposed by the Constitution of Canada which includes the Charter of Rights and Freedoms as well as federal criminal law provisions in relation to the interception of private communications.

So far as case law is concerned, the courts in Canada appear to have applied the law relating to monitoring and surveillance in a similar way to the courts in Europe. Therefore, key issues in relation to both video surveillance and GPS monitoring (recognising that such monitoring is intrusive) have been the address of a specific identified need - the need to be effective in meeting such need, balancing this with the loss of privacy involved and exploring whether there is a less invasive means of achieving the same end.

IT monitoring also requires notification to employees that monitoring may take place (with employee consent being advisable) but that even where obtained, a residual expectation of privacy will remain in relation to, for example, personal health records or very personal family correspondence, access to which would be viewed as a unreasonable search which cannot be justified.

Social media information even where publicly available is viewed as being subject to personal data protection legislation, such that employers must identify the purpose of which such information is collected and use it only for that purpose.

US

Commentary on existing case law

The US has no comprehensive national data privacy regime. Rather national legislation is addressed on a sectoral basis (health, financial bases, etc.). Some of the more liberal states, (e.g. California, New York, Massachusetts, Oregon, etc.) have stepped in to attempt to fill the void by affording more privacy protections on a state or even city basis. For the most part, even with additional state or city laws, data privacy in the United States is more limited than in the EU. Because data privacy consists of a patchwork of national, state and sometimes even municipal laws, one cannot assume that simply because a practice is permitted under federal law, or in one state, that it is permitted in another US state.

Trends that can be identified

Security breach laws have been adopted in all US states, except for Alabama and South Dakota. The Security and Exchange Commission has also indicated that it will look into enforcement actions against publicly traded companies which fail to properly safeguard their consumer or other personal data as it can dramatically impact shareholders given the proliferation of multi-million dollar class-action litigation such breaches can generate. "Ban the Box" legislation which has mushroomed among states and cities is currently being considered by the US Congress. Social media companies' role in society, including gun violence and election interference, is likely to lead to additional voluntary or legislatively mandated scrutiny of its platforms and usages. Given that under the Trump administration the NLRB has become considerably more conservative, we anticipate that the very broad social media "concerted activity" protections will be pulled back considerably.

Existing case law

California

1. *Rulon-Miller v.. IBM*, 162 Cal. App. 3d 241 (Cal. Ct. App. 1984) (page 153)
2. *Pettus v.. Cole*, 49 Cal. App. 4th 402 (Cal. Ct. App. 1996) (page 154)
3. *TBG Insurance Services Corp. v.. Superior Ct.*, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002) (page 155)
4. *Hernandez V.. Hillsides, Inc. et al.*, 47 Cal. App. 4th 272 (Cal. Ct. App. 2009) (page 156)
5. *Holmes v.. Petrovich Dev. Co., LLC*, 191 Cal. App. 4th 1047 (Cal. Ct. App. 2011) (page 157)
6. *Cochran v.. Schwan's Home Services Inc.*, 228 Cal. App. 4th 1137 (Cal. Ct. App. 2014) (page 158)

New York

1. *Bilquin v.. Roman Catholic Church*, 729 N.Y.S.2d 519 (N.Y. App. Div. 2001) (page 159)
2. *Scott v.. Beth Israel Med. Ctr., Inc.*, 17 Misc. 3d 934 (Sup. Ct. N.Y. Cty. 2007) (page 160)
3. *AllianceBernstein L.P. v. Atha*, 954 N.Y.S.2d 44 (N.Y. App. Div. 2012) (page 161)

Federal

1. *Watkins v.. LM Berry & Co.*, 704 F.2d 577 (11th Cir. 1983) (page 162)
2. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D. N.Y. 2005) (page 163)
3. *Pure Power Boot Camp v.. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (page 164)
4. *KLA-Tencor Corp. v.. Murphy*, 717 F. Supp. 2d 895 (N.D. Cal. 2010) (page 165)
5. *In Re the Reserve Fund Securities and Derivative*, 673 F. Supp. 2d 182 (S.D.N.Y. 2009) (page 166)
6. *Chamberlain v.. Les Schwab Tire Center Of California, Inc.*, No. 2:11-cv-03105-JAM-DAD, 2012 WL 6020103 (E.D. Cal. Dec. 3, 2012) (page 167)
7. *Simpson v.. Vantage*, No. 12-cv-04814-YGR., 2012 WL 6025772 (N.D. Cal. Dec. 4, 2012) (page 168)
8. *Hispanics United Of Buffalo, Inc. And Carlos Ortis*, 359 NLRB No. 37 (Dec. 14, 2012) (page 169)
9. *Sunbelt Rentals v.. Victor*, 43 F. Supp. 3d 1026 (N.D. Cal. 2014) (page 170)
10. *Pier Sixty, LLC*, 362 N.L.R.B. No. 59 (Apr. 21, 2017) (page 171)

California

Case Name, Citation and Court	<p>Rulon-Miller v.. IBM, 162 Cal. App. 3d 241 (Cal. Ct. App. 1984)</p> <p>Court of Appeal, First District, Division 1, California.</p>
Date	29 November 1984
Subject	Off Duty Conduct
Key facts	<ul style="list-style-type: none">• Rullon Miller (Plaintiff) was a sales representative for IBM (Defendant).• Rullon Miller was in a relationship with a former IBM sales representative, Blum, who left IBM to work for IBM's competitor. Rulon-Miller's manager inquired about her relationship with Blum, and Rulon-Miller asserted her right to privacy based on IBM's employment policies. Specifically, an IBM memorandum that said IBM was only concerned with an employee's off-the-job behavior if the behavior interfered with the employee's ability to perform or seriously affected the reputation of IBM.• IBM also had policies governing conflicts of interest. But IBM did not have a policy that specifically regulated romantic relationships with the employees of its competitors.• Rulon Miller's manager asserted that Rulon-Miller's relationship with Blum was a conflict of interest and terminated her employment with IBM. Rulon-Miller sued for wrongful discharge and intentional infliction of emotional distress. The jury in trial court found in favor of Rulon-Miller. IBM appealed.
Key points	<p>The Court of Appeal held that:</p> <ul style="list-style-type: none">• The conflict of interest allegation was a pretext for plaintiff's unjust termination. The record showed that IBM did not interpret its conflict of interest policy to prohibit a romantic relationship, and there was no company rule or policy requiring an employee to terminate friendships with fellow employees who leave and join competitors.• Further, Rullon Miler's position did not grant her access to sensitive information which could have been useful to competitors.• IBM's policies gave Rullon-Miller the right to privacy. Policy said "<i>IBM's first basic belief is respect for the individual, and the essence of this belief is a strict regard for his right to personal privacy. This idea should never be compromised easily or quickly.</i>"

Case Name, Citation and Court	Pettus v.. Cole, 49 Cal. App. 4th 402 (Cal. Ct. App. 1996) California Court of Appeal
Date	12 September 1996
Subject	Confidentiality of Medical Information
Key facts	<ul style="list-style-type: none"> • Employee (Plaintiff) requested stress-related disability leave. • In the course of having the disability request verified, employee submitted to two psychiatric evaluations arranged for and paid by his employer. • Without employee's consent, psychiatrists sent full written reports to employer. Reports contained information about employee's family and work histories, his drinking habits, emotional conditions, including his hostile feelings towards co-workers and employer. • As a result of the report, employer informed employee that he will be required to enroll in an inpatient alcohol treatment program in order to continue his employment. Employee refused and was terminated. • The court reviewed whether and to what extent medical information compiled during the psychiatric examination of an employee may be disclosed to the employer by a psychiatrist without employee authorization where the examination is required under the employer's short-term disability policy, and arranged and paid for by the employer.
Key points	<p>The court held that:</p> <ul style="list-style-type: none"> • Psychiatrists violated the Confidentiality of Medical Information Act (CMIA) by providing employer a detailed report of employee's psychiatric examinations without written authorization. • Psychiatrists violated employee's state constitutional right of privacy (Cal. Const., Article I § 1) since employee had a legally cognizable interest in maintaining the privacy of highly sensitive, embarrassing and personal information, which he could reasonably expect to be confidential. • However, the Court of Appeal remanded for further review whether employee waived his constitutional rights by voluntarily disclosing to his supervisors much of the sensitive personal information that was subsequently transmitted in the psychiatrists' reports.

Case Name, Citation and Court	TBG Insurance Services Corp. v.. Superior Ct., 96 Cal. App. 4th 443 (Cal. Ct. App. 2002) California Court of Appeal
Date	22 February 2002
Subject	No reasonable expectation of privacy in an employer-owned computer located at employee's home
Key facts	<ul style="list-style-type: none"> Employer (Defendant) fired former employee (Plaintiff) because employee accessed pornographic websites while at work in violation of employer's electronic policies. Employee brought a wrongful termination action against employer. Employee was provided with two computers for use at work and for working at home. In signing employer's policy statement, he had agreed to use the computers only for business purposes. Employer moved to compel the employee to produce the home computer, but employee opposed the motion claiming that the computer contained personal information, and that production of the computer would invade his constitutional right of privacy. The trial court denied the motion.
Key points	<p>The appellate court held that:</p> <ul style="list-style-type: none"> Employee should produce the home computer because he had no reasonable expectation of privacy in an employer-owned computer although it was located at his home. Employer's advance notice to employee by way of the policy statement which he signed acknowledging that the home computer was the property of the Company and, as such, "<i>to be used for business purposes only and not for personal benefit or non-Company purposes</i>" defeated his claim of privacy. Employee understood that communications transmitted by Company systems were not considered private, and consented to employer's discretionary monitoring of its computer systems messages and files. Therefore, he knew that employer would monitor the files and messages stored on his home computer.

Case Name, Citation and Court	<i>Hernandez v.. Hillsides, Inc. et al., 47 Cal. 4th 272 (2009)</i> Supreme Court of California
Date	3 August 2009
Subject	Invasion of Privacy, workplace videotaping
Key facts	<ul style="list-style-type: none"> Employees (Plaintiffs) were employed by Hillsides, Inc. (Defendant) at a non-profit residential facility for abused children. Employees shared an enclosed office where they worked on computers during regular business hours. The director of Hillsides learned that someone was using an office computer to watch pornography. In an attempt to catch the unauthorized viewer, Hillsides installed a hidden remote operated camera in the employees' office. Hillsides never used the camera during the day or to tape the Employees. Employees brought an action for invasion of privacy against Hillsides after discovering the camera.
Key points	<ul style="list-style-type: none"> The Trial court held that there was no intrusion because the Employees were never actually videotaped. The Court of Appeal overturned, holding that the Employees met the elements of an invasion of privacy claim because they suffered an intrusion into a zone of privacy, and it was so unjustified and offensive as to constitute a privacy violation. The California Supreme Court disagreed and held that while the Employees had suffered an intrusion into a zone of privacy, no reasonable jury could find that the intrusion was unjustified or offensive. The Supreme Court held that the Employees had a reasonable expectation of privacy because privacy is heightened in enclosed offices where an employee does not expect to be overheard or observed, in contrast to a large cubicle environment on one end providing very low expectations of privacy. Also, the use of a videotape was subject to a high standard because it is so invasive, and Employees had no notice that they may be subject to surveillance. Nonetheless, the California Supreme Court held that there was no invasion of privacy because Hillside's surveillance was limited in scope; the camera never actually recorded the Employees; surveillance was conducted for a legitimate purpose and only after work hours.

Case Name, Citation and Court	Holmes v.. Petrovich Dev. Co., LLC, 191 Cal. App. 4th 1047 (Cal. Ct. App. 2011) California Court of Appeal
Date	13 January 2011
Subject	Privileged electronic communications with attorney transmitted in violation of employer's email policy is not protected Attorney Client Privilege
Key facts	<ul style="list-style-type: none"> • Employee sued employer for sexual harassment, and a number of other claims arising from the sexual harassment claim. • Employee used her work computer to send emails via her private email account to her attorney regarding the various claims. • Employee argued that she had a reasonable expectation of privacy because she utilized a private password to use her employer's computer and deleted the emails after they were sent, and no one had asked or knew her password, and the company rarely monitored or audited employee's use of its computers in compliance with the policy.
Key points	<p>The Court denied employee's assertions and held that:</p> <ul style="list-style-type: none"> • The emails were not protected by the attorney-client privilege because (i) employee was aware of the company's policy prohibiting employees from sending or receiving personal email via its systems: (ii) employee had been warned that the company would monitor its computers for compliance with randomly and its discretion; (iii) employer "<i>explicitly told employees that they did not have a right to privacy in personal email sent by company computers, which email the company could inspect at any time at its discretion, and the company never conveyed a conflicting policy.</i>" • By communicating through her work computer despite knowing the emails violated company policy and the company could examine the messages at any time, the employee could not reasonably have expected that the communication would remain private. Therefore, they were not privileged.

Case Name, Citation and Court	<i>Cochran v.. Schwan's Home Services Inc., 228 Cal. App. 4th 1137 (Cal. Ct. App. 2014)</i> California Court of Appeal
Date	12 August 2014
Subject	BYOD, reimbursement for use of personal cell phone for work-related purposes
Key facts	<ul style="list-style-type: none"> Putative class action against employer seeking reimbursement for expenses pertaining to work-related use of employee personal cell phones. Issue before the court was whether an employer must always reimburse an employee for the reasonable expense of the mandatory use of a personal cell phone, or whether the reimbursement obligation is limited to the situation in which the employee incurred an extra expense that he or she would not have otherwise incurred absent the job.
Key points	<ul style="list-style-type: none"> The court held that California labour law requires employers to reimburse employees who are required to use their personal cell phones for work-related purposes for a reasonable percentage of their cellphone bill. The reimbursement obligation is triggered regardless of whether employees incur any additional expense.

New York

Case Name, Citation and Court	<i>Bilquin v.. Roman Catholic Church, 729 N.Y.S.2d 519 (N.Y. App. Div. 2001)</i> New York Appellate Division
Date	20 August 2001
Subject	Off Duty Conduct, what is a recreation activity?
Key facts	<ul style="list-style-type: none">• Employer refused to renew employee's contract of employment because she was cohabiting with a man who was married to another woman.• Employee sued for wrongful termination of employment claiming that the termination of her employment violated section 201-d(2)(c) which bars an employer from discharging an employee because of the employee's legal recreational activities outside work hours.
Key points	The court held that: <ul style="list-style-type: none">• Employee's conduct did not constitute a recreational activity within the meaning of section 201-d(2)(c).

Case Name, Citation and Court	<i>Scott v.. Beth Israel Med. Ctr., Inc., 17 Misc. 3d 934 (Sup. Ct. N.Y. Cty. 2007)</i> New York Superior Court
Date	17 October 2007
Subject	Privileged electronic communications with attorney transmitted in violation of employer's email policy is not protected Attorney Client Privilege
Key facts	<ul style="list-style-type: none"> • Former employee (Plaintiff) sued employer (Defendant) for breach of contract. • Employee sought the return of email correspondence with his lawyer that was in possession of his former employer on the basis that the documents were privileged communications belonging to employee and for which there had been no waiver of privilege. • Employer refused to return the emails and argued that the emails were never protected by the attorney-client privilege because employee had no reasonable expectation of privacy when using his former employer's computer system in violation of the employer's email policy. Consequently, employee waived the attorney-client privilege.
Key points	<p>The court held that:</p> <ul style="list-style-type: none"> • Employee had waived the attorney-client privilege by using his employer's computer systems. • Employer's "no personal use" email policy and policy allowing employer to monitor its computer system diminished any reasonable expectation of privacy. • Employer's policy provided in relevant part that all of the employer's computer systems . . . "<i>should be used for business purposes only.</i>" All information and documents created, received, saved or sent on employer's computer or communications systems "<i>are [company] property,</i>" and that "<i>employees have no personal privacy right in any material created, received, saved or sent using [employer's] communications and computer systems.</i>" Employer's policy also stated that employer "<i>reserves the right to access and disclose such material at any time without prior notice.</i>" • As a result of the clear language of the policy, employee had no reasonable expectation of privacy.

Case Name, Citation and Court	AllianceBernstein L.P. v. Atha, 954 N.Y.S.2d 44 (N.Y. App. Div. 2012) Supreme Court, Appellate Division, First Department, New York
Date	15 November 2012
Subject	Bring Your Own Device (BYOD)
Key facts	<ul style="list-style-type: none"> Employer sued a former employee on the basis that the employee had breached his employment agreement by, among other things, stealing its confidential client contact data so that he could solicit its clients at his new firm. Employer sought and received a Temporal Restraining Order (TRO) against employee which stopped him from using the stolen information. The employer sought discovery of employee's personal iPhone, arguing that employee had serviced its clients over that phone and the device contained the contact information of it's clients.
Key points	<ul style="list-style-type: none"> The trial court granted employer's request for a TRO and directed employee to hand over his iPhone so that the employer could obtain the contact information it requested. The appellate court in an attempt to balance the privacy and commercial interests of the employee against the need for relevant information sought by the employer, reversed the order, holding that requiring production of the entire iPhone was too invasive. The appellate court ordered the phone to be reviewed in camera to ensure that only relevant, non-privileged information would be disclosed. The court reasoned that ordering the production of defendant's iPhone, which has built-in applications and internet access, is equal to ordering the production of his personal computer which would be improper.

Federal

Case Name, Citation and Court	<i>Watkins v.. LM Berry & Co.,704 F.2d 577 (11th Cir. 1983)</i> Eleventh Circuit
Date	2 May 1983
Subject	Federal Wiretapping Statute, Interception of Phone Conversations
Key facts	<ul style="list-style-type: none">• Employee worked for employer selling advertising by telephone.• Employer had an established policy of monitoring solicitation calls as part of its regular training program.• Employer allowed employees to make personal calls and were not told whether those calls would be monitored.• A friend called employee at work about a new job, and employer monitored the call.• Employee sued employer alleging violation of federal wiretapping statute arising out of employer's monitoring of her personal telephone call.• Employer argued that employee's acceptance of employment which included knowledge of employer's monitoring policy constituted her consent to the interception of her personal call.
Key points	The Court, interpreting federal law, held that: <ul style="list-style-type: none">• It was not clear that employee consented to the interception of personal calls because employee did not consent to a policy of general monitoring. Employee consented to a policy of monitoring sales calls but not personal calls. Court reasoned that employee's consent included the inadvertent interception of a personal call, but only for as long as necessary for her employer to determine the nature of the call.• Therefore, once an employer realizes the call is personal, he or she must immediately stop monitoring the call. Here the court held that if employer's interception went beyond the point necessary to determine the nature of the call, it went beyond the scope of employee's actual consent.

Case Name, Citation and Court	<i>In re Asia Global Crossing, Ltd., 322 B.R. 247 (Bankr. S.D. N.Y. 2005)</i> Southern District, New York, Bankruptcy
Date	21 March 2005
Subject	Privilege communication on employer owned devices.
Key facts	<ul style="list-style-type: none"> • Employer filed for bankruptcy under Chapter 1 and a Trustee was appointed. Employer had five principal corporate officers (the Insiders). • Insiders' counsel learned that allegedly privileged emails and privileged hard copy documents had been left behind when the Trustee ordered the premises vacated, and asked Trustee's counsel to keep the Insider emails and hard copy documents confidential. The documents were segregated and held. • Trustee began an investigation into certain transactions involving the Insiders and requested the production of documents. The Insiders refused to produce the emails and hard copy documents on the basis of privilege. • The Trustee issued a second subpoena which specifically requested production of any electronic document generated or received on former employer's computer systems, and any hard copy documents which were located at employer's premises at the time of the conversion to chapter 7. The Insiders again refused to produce and argued attorney-client privilege.
Key points	<p>The court held that:</p> <ul style="list-style-type: none"> • Assuming that an email is otherwise privilege, the use of an employer's email system does not without more destroy privilege. • The Insider's use of the employer's system to communicate with their personal attorneys did not eliminate any existing attorney-client privilege because evidence of the existence of a corporate policy banning personal use of email and allowing monitoring was ambiguous. • The court rejected the Trustee's argument that the Insiders waived any privilege attached to the hard copy documents because they abandoned the documents at former employer's premises and some of the documents may have been generated and stored on employer's computers on the basis that the hard copy documents were inadvertently left behind. Therefore privilege was maintained.

Case Name, Citation and Court	Pure Power Boot Camp v.. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) Southern District, New York
Date	23 October 2008
Subject	Review of personal emails maintained by outside electronic communication service providers like Hotmail on employer-issued device.
Key facts	<ul style="list-style-type: none"> Employer (Defendant) accessed former employee's (Plaintiff) Hotmail account because employee left his password and username information stored on employer's computer. Employee claimed that his former employer's review of his Hotmail emails was unauthorized and illegal under the Stored Communications Act (SCA). Employer argued that its review of employee's emails did not violate the SCA because (i) employer's email policy put employee on notice that his emails could be viewed by employer, and (ii) employee leaving his username and password on his employer's computer system gave implied consent to access his accounts.
Key points	<p>The Court held that:</p> <ul style="list-style-type: none"> Employee did not store any of the communication which employer accessed on the employer's computers, servers, or systems, nor were any of the emails sent from or received on the employer's company email system. The Court stressed that this was not a situation where the employer was attempting to use emails obtained from its own computers or systems. To hold that an employee by inadvertently leaving his Hotmail password accessible on his work computer authorized his employer to access his Hotmail emails will be tantamount to arguing that if the employee had left his house keys on the reception desk at the office, he would have been implicitly authorizing his employer to enter his home without his knowledge. Further, employer's company policy did not provide the necessary authorization because it only referred to communications sent over its systems.

Case Name, Citation and Court	KLA-Tencor Corp. v.. Murphy, 717 F. Supp. 2d 895 (N.D. Cal. 2010) Northern District, California
Date	11 May 2010
Subject	Federal Wiretapping Statute
Key facts	<ul style="list-style-type: none"> Employer brought action against its former employee and competitor, asserting claims for, inter alia, trade secret misappropriation against competitor, and claims for violations of the Computer Fraud and Abuse Act (CFAA) and Electronic Communications Privacy Act (ECPA). The SCA creates a private cause of action for persons aggrieved by violations of the ECPA. Employer argued that employee violated the CFAA by using a program called Evidence Eliminator to delete all of her email accounts and files on her laptop prior to leaving employer's firm. Employer argued that employee's access to the computer was not authorized. Employer relied on its employee agreement which required the surrender of all proprietary information upon termination of employment to mean that employees were not authorized to delete confidential information residing on their computers.
Key points	<p>The court held that:</p> <ul style="list-style-type: none"> Deletion of documents and emails among other items, constitutes "<i>damage</i>" under the CFAA, but in this case employer did not present sufficient evidence to show damage since employee only accessed proprietary information and did not damage any systems or destroy any data. Court reasoned that employee's deletion of the files did not deprive employer of them since the files still remained available elsewhere. The court also held that employee did not violate the SCA because it was not clear that the emails on employee's server were in electronic storage as conceived by the SCA, there was no evidence that employee acted intentionally, and it appeared that employee's conduct was authorized because employees were generally authorized to use their own cell phones.

Case Name, Citation and Court	<i>In Re the Reserve Fund Securities and Derivative, 673 F. Supp. 2d 182 (S.D.N.Y. 2009)</i> Southern District, New York
Date	23 May 2011
Subject	Privacy, no reasonable expectation of privacy in an employer-owned computer
Key facts	<ul style="list-style-type: none"> Plaintiff sought to recover email communications made between defendant and his wife. Defendant refused to produce the emails and argued that the email communications between himself and his wife were protected by the marital communications privilege. Plaintiff argued that defendant had no reasonable expectation of privacy in the emails because he transmitted them over his employer's system and the emails were stored on his employer's server.
Key points	<p>The Court held that:</p> <ul style="list-style-type: none"> Defendant had no reasonable expectation of privacy in the emails he sent to his wife over his employer's computer system, therefore they were not "<i>in confidence</i>" and were not protected by the marital communications privilege. Employer's policy (1) limited email use of computer systems to business purposes and banned personal use, (ii) employer reserved the right to access or inspect its employees' emails or work computers, (iii) employer's policy explicitly warned employees that their email communications will be automatically saved and are subject to review by employer and disclosure to third parties, and (iv) Defendant was aware of company's email policy.

Case Name, Citation and Court	<i>Chamberlain v.. Les Schwab Tire Center Of California, Inc., No. 2:11-cv-03105-JAM-DAD, 2012 WL 6020103 (E.D. Cal. Dec. 3, 2012)</i> California District Court
Date	3 December 2012
Subject	Cal Labor Code 632; nonconsensual recording of phone conversations.
Key facts	<ul style="list-style-type: none"> • Plaintiff was laid off when Defendant closed the shop where Plaintiff worked. • When Defendant closed shop it encouraged the employees working at that store to contact other stores in the chain to find another position. • Plaintiff alleges that he was not hired by another store in the chain because he could not work on Saturdays due to his religious observation of the Sabbath. In support of his claim, Plaintiff referred to three conversations that he had with Defendant's employees who managed a local store for Defendant. • Defendant argued that Plaintiff's actions violated Cal. Lab. Code 632 which prohibits eavesdropping or intentionally recording a confidential communication without the consent of all parties to the communication. • Plaintiff argued that his recordings were not illegal because they occurred in public spaces and could be easily overheard. His conversations took place in open spaces where other employees were coming and going and could easily overhear his conversations.
Key points	<p>The Court held that:</p> <ul style="list-style-type: none"> • <i>"Because the conversations occurred in public places with people around, the Court finds that [defendant] had no reasonable expectation that their conversations would not be overheard or recorded."</i>

Case Name, Citation and Court	Simpson v.. Vantage, No. 12-cv-04814-YGR., 2012 WL 6025772 (N.D. Cal. Dec. 4., 2012) Northern District, California
Date	4 December 2012
Subject	Interception of Phone Conversations
Key facts	<ul style="list-style-type: none"> Plaintiff brought a class action for violation of California Penal Code section 632.7 against Defendant. Plaintiff alleged Defendant unlawfully recorded conversations between the parties in violation of Section 632.7 which prohibits the use of “<i>an electronic tracking device to determine the location or movement of a person</i>” via a “<i>vehicle or other moveable thing</i>” unless “<i>the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle</i>.” Defendant made two arguments in support of its motion to dismiss: (1) Section 632.7 “<i>does not apply to participants of a telephone conversation because the statute targets unauthorized eavesdropping or a recording of conversations by third parties</i>,” i.e. 632.7 does not apply to the parties of a call, and (2) Section 632.7 protects only “<i>confidential</i>” communications in circumstances where there is a reasonable expectation of privacy.
Key points	<p>The Court held that:</p> <ul style="list-style-type: none"> 632.7 applies to parties of a call. While the common understanding of the word “<i>intercepts</i>” contemplates the existence of a third party, the word “<i>receives</i>” in the section shows the provision’s applicability to call participants under the reasoning that during a call the participants “<i>receive</i>” communications from each other. The Court also rejected Defendant’s argument that Section 632.7 only applies to “<i>confidential</i>” communications as contrary to the plain meaning of the statute.

Case Name, Citation and Court	<i>Hispanics United Of Buffalo, Inc. And Carlos Ortis, 359 NLRB No. 37 (Dec. 14, 2012)</i> National Labor Relations Board
Date	14 December 2012
Subject	Social Media postings
Key facts	<ul style="list-style-type: none"> Five employees (Plaintiffs) posted comments on Facebook in response to a co-workers criticism of their job performance. Plaintiff received a text message from a co-worker in which the co-worker said she intended to discuss her concerns regarding employee performance with the Director (Lourdes). In response, Plaintiff questioned whether the co-worker really "wanted Lourdes to know ... how u feel we don't do our job..." Plaintiff then posted the following message on her Facebook page: "<i>Lydia Cruz, a coworker feels that we don't help our clients enough at [Hispanics United of Buffalo Inc.]. I about had it! My fellow coworkers how do u feel?</i>" The four other Plaintiffs responded by posting messages, via their personal computers, on Plaintiff's Facebook page objecting to the assertion that their work performance was substandard. The co-worker responded and asked Plaintiff to "stop with ur lies about me." The employer discharged all five employees stating that their behavior constituted bullying and harassment of a co-worker in violation of the company's zero tolerance policy prohibiting such conduct. Issue before the National Labor Relations Board (NLRB) was whether Facebook communications were "<i>protected concerted activity</i>" within the meaning of Section 7 of the NLRA Act, which guarantees non-supervisory employees' right to engage in concerted activities for the purpose of collective bargaining or other mutual aid or protection.
Key points	<ul style="list-style-type: none"> The NLRB Board held that the employer violated the Act because the Facebook communications were a protected concerted activity. The conversations were about employees' job performance, and terms and conditions of employment, and the actions were concerted because it could be perceived as employees' first step towards taking group action to defend themselves against accusations of poor job performance. Per the NLRB, the employees' Facebook comments could not reasonably be perceived as a form of harassment or bullying within the meaning of the employer's policy.

Case Name, Citation and Court	<i>Sunbelt Rentals v.. Victor, 43 F. Supp. 3d 1026 (N.D. Cal. 2014)</i> Northern District, California
Date	28 August 2014
Subject	Employer's ability to access text messages stored in company issued device; invasion of privacy - hacking, does a text message stored in a cellular telephone constitute electronic storage for purposes of the SCA?
Key facts	<ul style="list-style-type: none"> • Company sued former employee for misappropriating trade secrets when it discovered, upon employee's termination, a number of text messages on the former employee's company-issued iPhone that documented his misappropriation. • Employee had forgotten to delink his Apple account from the company phone he returned, and thus, his text messages continued to go to the phone, and his former employer. • Employee alleged that employer violated the SCA by reviewing his text messages; invaded his privacy under California Penal Code § 630 and wrongfully accessed his post-employment electronic data communications without his knowledge and consent in violation of California Penal Code § 502
Key Points	<p>The Court rejected all arguments and held that:</p> <ul style="list-style-type: none"> • SCA was not applicable because text message and pictures stored on a cellular telephone do not constitute electronic storage for purposes of the SCA. • There was no invasion of privacy because employee had no reasonable expectation of privacy in a company-owned phone that was no longer in his possession. Phone belonged to employer and employee caused the transmission of the text messages to device owned by employer. • Employee did not allege enough facts to show that employer hacked into his electronic data and communications by circumventing technical or code based barriers intended to restrict such access. Indeed, employer gained access to text messages because employee inadvertently failed to unlink his former company phone from his iPad when he synced his new devices to his iPad.

Case Name, Citation and Court	Pier Sixty, LLC, 362 N.L.R.B. No. 59 (Apr. 21, 2017) National Labor Relations Board and Second Circuit
Date	21 April 2017
Subject	Employee Facebook Posts, National Labor Relations Board
Key facts	<ul style="list-style-type: none"> Prior to an election to unionize, employee posted a message on his Facebook page using profanity about his supervisor, and his supervisor's family, and encouraging employees to vote yes for the union. Employee's post read "<i>Bob is such a NASTY MOTHER F***er, don't know how to talk to people!!!!!! F**k his mother and his entire f***ing family!!!! What a LOSER!!!! Vote YES for the UNION!!!!!!</i>" Employee took down the post three days later but it had already come to the attention of management which, following an investigation, fired employee. Employee filed a charge with the National Labor Relations Board (NLRB) claiming he had been terminated in retaliation for "<i>protected concerted activities</i>" under the National Labor Relations Act (NLRA).
Key points	<ul style="list-style-type: none"> The NLRB found that employee's activity was protected under NLRA sections 8(a)(1) and (a)(3) and his termination was in retaliation for "<i>protected concerted activities</i>." Employer filed a petition for review before the second circuit. The second circuit affirmed the NLRB's determination that employer violated Sections 8(a)(1) and 8(a)(3) by terminating employee. The Court held that employee's conduct was not so "<i>opprobrious</i>" as to lose the protection of the NLRA. But the court noted that employee's behavior sits at the outer-bounds of protected, union-related comments.

Summary of existing legislation

California

California has a Constitutional right of privacy in its First Amendment applicable to the private sector.

California Penal Code Section 632 makes it a crime to use electronic amplification or a recording device to listen in to someone's conversation without all parties' consent.

California Penal Code Section 632.5 and 623.6 make it a crime to intercept a call from a cell phone or cordless phone, or intercept or receive communications between a cell phone or landline and a cordless phone, respectively, without the consent of all parties.

California Labor Code 1102 prohibits coercion or attempt to coerce or influence an employee through or by means of threat of discharge to adopt or follow or refrain from adopting any particular course or line of political action or political activity.

California Labor Code 232 and 232.5 prohibit the employer from restricting employee discussion regarding wages and terms and conditions of employment.

California Labor Code 432.5 prohibits inquiry into an applicant's or employee's prior compensation history.

California Labor Code 980 prohibits an employer from requesting access to a job applicant's social media, except in limited circumstances.

California Labor Code §§ 96(k), 98.6 prohibits the discharge or discrimination in employment based on "*lawful conduct occurring during nonworking hours away from the employer's premises.*"

California Penal Code section 637.7 prohibits the use of "*an electronic tracking device to determine the location or movement of a person*" via a "*vehicle or other moveable thing*" unless "*the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle.*"

New York

New York Penal Law 250.00(1) prohibits the intentional overhearing or recording of a telephonic or telegraphic communication by a person other than a sender or receiver thereof without the consent of either the sender or receiver, by means of any instrumenting, device or equipment.

New York Labor Code § 201-d(2)(c) prohibits discrimination against an employee for his or her participation in "*legal recreational activities outside work hours.*"

New York Labor Code §194.4 prohibits the employer from restricting employee discussion regarding wages and terms and conditions of employment. This provision also prohibits an employer from inquiring into an employee's prior compensation history until after an employment offer has been made.

Federal

Computer Fraud and Abuse Act (**CFAA**) makes it a federal crime to access a protected computer without proper authorization.

Electronic Communications Privacy Act (**ECPA**) is a federal statute that prohibits a third party from intercepting

or disclosing communications without authorization.

Stored Communications Act (**SCA**) protects personal information stored by electronic communication service providers and remote computing service providers.

Future legislation which may have an impact on employee monitoring

We are not aware of any impending legislation that may impact on employee IT monitoring.

Canada

Commentary on existing case law

Most Canadian decisions on employee monitoring have been issued by privacy commissioners pursuant to Canada's federal or provincial data protection legislation. The cases have focused on balancing employers' legitimate interests including productivity, safety and asset protection against the privacy rights of employees. The privacy commissioner rulings have been fairly consistent. In addition, a number of union arbitrators have addressed video surveillance and other types of workplace surveillance, generally following the same principles as the privacy commissioners, but in the context of any specific collective bargaining agreement provisions. This report focuses on the common law jurisdictions of Canada – i.e. the federal sphere and all territories and provinces with the exception of the Province of Québec.

In addition, the top appellate court of the Province of Ontario has fairly recently recognized something akin to a tort of invasion of privacy, calling it "*intrusion upon seclusion*". While the case law has not yet developed significantly, one can fairly anticipate that there will be further claims for tort damages.

The privacy commissioners have created the framework of Canada's case law to date. When looking at biometrics scanning systems, the privacy commissioner's decisions have typically addressed whether the collection, use or disclosure of the personal characteristics (for example, voice prints, handprints or fingerprints) was only for purposes that a reasonable person would consider to be appropriate in the circumstances. The commissioners and courts have looked at the degree of sensitivity associated with the biometric information, the employer's security measures, the bona fide business interest of the employer, the effectiveness of the use of biometrics to meet those objectives, the reasonableness of the collection of the biometric data measured as against alternative methods of achieving the same levels of security at comparable costs and with comparable benefits, and the proportionality of the loss of privacy as against the cost and operational benefits for the employer. The cases often look at whether the collection of data, therefore, would be seen by a reasonable person to be appropriate in the circumstances. Employee consent is obtained when employees enroll in the biometric system.

Certain provincial legislation permits collection of employee personal information without consent if the collection is reasonable for the purposes, the information is related to the employment and the employer has provided the individual with reasonable notification of the collection and of the purpose. Therefore, the Canadian cases vary with respect to the need for explicit employee consent.

In the situations involving monitoring of computer usage and emails, consent was less frequently sought, as many of these cases involve surreptitious monitoring by the employer. The cases have varied as to whether what an employee produces on the computer is work product or personal data about the creator. A number of cases have found that the employees' productivity and production on a work computer constitutes the personal data of the employee and, therefore, is protected under the data protection legislation. The question has not been fully resolved at this point. Certain legislation also permits an organization to collect personal data without knowledge or consent in a number of situations including where it is reasonable to expect that collection with knowledge or consent would compromise the availability or the accuracy of the data, or where the collection is reasonable for purposes relating to investigation of a breach of an agreement or a contravention of the laws of Canada.

Certain privacy commissioner rulings have indicated that, even where emails sent or received by employees on an employer system are considered to be corporate records, the emails are also the employees' personal

information and protected by data protection legislation. For this reason, the privacy commissioners have required employers which monitor employee email to have a justification for doing so. Employers should also have a workplace policy that makes it clear that monitoring may occur.

A key concern of privacy commissioners in such cases is whether the employer has exceeded what is reasonable. For example, in one case the employer was determined to have a legitimate reason for surreptitiously tracking an employee's internet activity. The concern in that case was that the employee seemed to be spending an excessive amount of time accessing the internet during working hours, which was affecting his productivity and timeliness. The employer went further by installing software which collected a record every two minutes and took a screen shot. While the employer disabled the keystroke tracking function so as not to record any of the employee's passwords, bank account numbers or other sensitive information that was not necessary for its investigation, the screen shot function did collect certain personal correspondence and banking information. The privacy commissioner determined that the screen shots constituted personal information about the employee and it was not necessary for the employer to go so far as to install the screen shot spyware. There were less intrusive methods of monitoring to determine whether the employee was accessing non-work-related websites and how much time he was spending doing so. The employer should have tried to conduct other types of investigations or have questioned the employee before progressing to surreptitious collection of data. The employer was not able to show that alternative methods of addressing the problem would not have been effective.

The privacy commissioner rulings on GPS and video surveillance generally apply the same four-part test in determining whether the data collection is justified:

1. Is the measure demonstrably necessary to meet a specific need?
2. Is it likely to be effective in meeting that need?
3. Is the loss of privacy proportional to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?

While use of GPS for reasons such as management of assets and safety has been found to be acceptable, the privacy commissioners have shown concern over "*function creep*" due to concerns that employee performance management and discipline may be the objectives of the use of GPS monitoring.

Finally, some complaints have been received by the privacy commissioners involving recording of employee telephone conversations or surreptitious recording of employees. Recording an employee's conversation has been held to constitute collection of personal data about the employee. While the cases have not proceeded on the merits for various reasons, the privacy commissioners have made a number of recommendations about how recording should occur. Specifically, the employer should inform its employees of its plans to install recording equipment, inform employees why the equipment is being installed and implement a written workplace policy.

Generally, covert rather than overt surveillance is difficult to justify where a privacy complaint is filed. Generally speaking, covert surveillance would only be permissible where it is reasonable to expect that collection with knowledge or consent of the employee would compromise the availability of the information or the accuracy of the information. Surreptitious collection of data must be reasonable and related to investigating a breach of an employment agreement or contravention of breach of law. Any employer planning to use any form of technology for scanning or tracking employees or for surveillance must be able to show a clear business need that cannot be easily met in another less intrusive fashion.

Trends that can be identified

In 2012 an appellant court in Canada recognized a right of action akin to invasion of privacy. Until that time, such a tort had not been clearly recognized. The Court referred to this as the tort of intrusion upon seclusion and, to date, we have not had any significant development in this area, although we anticipate further case law. Intrusion upon seclusion can lead to damages but the intrusion needs to be a deliberate and significant invasion of personal privacy and needs to be objectively regarded as highly offensive. The Court indicated that this would include intrusion into one's financial or health records and into one's employment matters. We anticipate further developments in this area.

The video surveillance case law has been fairly well established since 2004. Video surveillance by an employer is regarded as intrusive and it must be directed at meeting a specific, identified need and needs to be effective in meeting such need. The need cannot be trivial, as there is a balancing between the loss of privacy as against the benefit to be gained by the surveillance. As with other types of surveillance in Canada, the employer needs to explore whether there is a less invasive manner of achieving the same end. In other words, most forms of surveillance, particularly video surveillance and the use of GPS data need to be a last resort for an employer.

The case law is fairly consistent with respect to the use of global positioning systems monitoring (**GPS**). Once again, the same test as in the case of video surveillance needs to be met – i.e. it is necessary to meet a specific need; likely to be effective; the benefit gained justifies the loss of privacy, and there is no less privacy invasive manner to achieve the same end. However, with GPS data, which can monitor employees' off-duty conduct, various privacy commissioner rulings have focused on a concern over possible use of the data for purposes other than the purpose for which it was originally collected. Any such additional use will be viewed as a breach of the legislative requirements.

In order to monitor the use of work email on workplace systems, the employer needs to notify employees that monitoring may take place. Employee agreement is advisable. Even where there is employee consent to monitoring, if email monitoring breaches the residual expectation of privacy (for example by looking at personal health records, very personal family correspondence, etc.) this would be viewed as an unreasonable search which cannot be justified by an employer.

Viewing social media information posted by an employee is viewed as collection of personal information subject to Canadian personal data protection legislation even though the data is publicly available. Therefore, employers need to identify the purpose for which they are collecting such data and use the data only for the purposes for which it was collected.

Existing case law

1. *Inappropriate monitoring of employees' email accounts*, Commissioner's Findings *Privacy Act*, January 29, 2003 (page 179)
2. *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 11 June 2004 (page 180)
3. *Government has right to monitor use of its email systems*, Commissioner's Findings *Privacy Act*, June 20, 2006 (page 181)
4. *Chatham-Kent (Municipality) v. CAW-Canada, Local 127*, 2007 CarswellOnt 5078 (page 182)
5. *Jones v. Tsige*, 2012 ONCA 32 (page 183)
6. *PIPEDA Case Summary #2006-351 – Use of personal information collected by Global Positioning System considered*, November 30, 2006 (page 184)
7. *R v. Cole*, 2012 SCC 53 (page 185)
8. *Schindler Elevator Corp., Re*, 2012 BCIPC 25 (page 186)
9. *Kone Inc.*, 20213 BCIPC No. 23 (page 187)
10. *R v. Mills*, 2013 CarswellNfld 431 (page 188)
11. *Toronto (City) v. Toronto Professional Fire Fighters' Association, Local 3888*, 2013 CanLII 76886 (ON LA) (Bowman Grievance) (page 189)
12. *SGEU and Unifor, Local 481 (Admissibility), Re*, 2015 CarswellSask 278 (page 190)
13. *Video surveillance of employees vs. right to privacy – a delicate balance*, Commissioner's Findings *Privacy Act*, December 10, 2015 (page 191)
14. *ATU, Local 113 v. Toronto Transit Commission*, 2017 ONSC 2078 (page 192)

Case Name, Citation and Court	<i>Inappropriate monitoring of employees' email accounts, Commissioner's Findings</i> Office of the Privacy Commissioner of Canada
Date	29 January 2003
Subject	Government monitoring of employees' personal emails
Key facts	<ul style="list-style-type: none"> • Two employees of Immigration and Refugee Board (IRB) alleged management improperly retrieved copies of confidential emails they had written each other. • IRB did not have a formal policy on the use of electronic networks at the time.
Key points	<ul style="list-style-type: none"> • The email messages between the two employees were personal in nature. • OPC found that the primary reason IRB retrieved the email messages was to conduct an internal disciplinary inquiry, it was not based on any concern that employees were improperly using the system. • It was unnecessary for IRB to retrieve the email exchanges to determine if disciplinary action against the employee was warranted. • IRB's actions not justified under the Privacy Act.

Case Name, Citation and Court	<i>Eastmond v. Canadian Pacific Railway, 2004 FC 852</i> Federal Court
Date	11 June 2004
Subject	Employer use of video surveillance in the workplace
Key facts	<ul style="list-style-type: none"> • CP installed six digital video recording surveillance cameras in its maintenance yard in Toronto to address CP's concerns regarding safety, security and potential liability. • Union filed a grievance to have the surveillance cameras removed on the basis it violated the collective agreement. • Recorded images were kept under lock and key and only accessed by responsible manager and CP police if there was an incident reported.
Key points	<ul style="list-style-type: none"> • Court found that the loss of privacy was minimal in proportion to the benefit gained from the collection of data and consent was not required to collect information. • The court applied the four-part test developed by the Privacy Commissioner of Canada: <ul style="list-style-type: none"> i. is the measure demonstrably necessary to meet a specific need? ii. is it likely to be effective in meeting that need? iii. is the loss of privacy proportional to the benefit gained? iv. is there a less privacy-invasive way of achieving the same end? • A person who might be recorded in the CP yard would have a low expectation of privacy since cameras were in a public space where collection was not surreptitious and warning signs were displayed. • A reasonable person would consider CP's purposes for collecting images of employees and others as appropriate under the circumstances.

Case Name, Citation and Court	<i>Government has right to monitor use of its email systems, Commissioner's Findings Privacy Act</i> Office of the Privacy Commissioner of Canada
Date	20 June 2006
Subject	Government's right to monitor employee use of its email systems
Key facts	<ul style="list-style-type: none"> • Canadian Border Services Agency (CBSA) computer system had online statement that employees had to agree to in order to gain access. • Online statement indicated CBSA may monitor the use of its systems, including email. • Normal routine analysis does not involve reading content. • If there is reasonable suspicion an individual is misusing the network, an investigation may involve reading content.
Key points	<ul style="list-style-type: none"> • OPC concluded that CBSA displayed fairness and transparency by informing employees of its monitoring practices through online statement and made the policy readily available • Governmental departments must conduct active monitoring and internal audits of security programs and electronic networks may be monitored • CBSA employees have clear expectations of the level of privacy they can expect from the employer

Case Name, Citation and Court	<i>Chatham-Kent (Municipality) v. CAW-Canada, Local 127, 2015 CarswellOnt 5078</i> Ontario Arbitration
Date	26 March 2007
Subject	Termination of employee based on personal blog
Key facts	<ul style="list-style-type: none"> • Employee was terminated by the Municipality for breaching the confidentiality agreement, insubordination and for conduct unbefitting of a Personal Care Giver at an old age home where she worked. • Employee had a personal blog where she published resident information and pictures without consent and made inappropriate comments about residents in her care and about management. • Termination was upheld despite eight years of service.
Key points	<ul style="list-style-type: none"> • Employee believed she had set up a private MSN Spaces website but it was available to anyone with an internet connection. • Employer had just cause to terminate employee because: <ul style="list-style-type: none"> ○ she was clearly in breach of confidentiality agreement by publishing personal information of residents online; ○ she was making insubordinate remarks about management; and ○ her comments and hostility demonstrated disregard for residents' need for care.

Case Name, Citation and Court	Jones v. Tsige, 2012 ONCA 32 Ontario Court of Appeal
Date	18 January 2012
Subject	New “ <i>intrusion upon seclusion</i> ” tort in Ontario; tortious invasion of privacy
Key facts	<ul style="list-style-type: none"> D was a bank employee who used her position to access her ex-spouse's current partner's (P) private bank records at least 174 times over a two-year period without professional justification. Novel tort of “<i>intrusion upon seclusion</i>” is accepted in Ontario and damages of \$10,000 were awarded.
Key points	<ul style="list-style-type: none"> The elements of “<i>intrusion upon seclusion</i>” include: (1) D's conduct must be intentional and reckless; (2) D must have invaded the private affairs of P without lawful justification and; (3) a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish. Proof of harm to an economic interest is not an element to the tort. In considering offensiveness, some factors include: degree of intrusion, context, conduct and circumstances of the intrusion, motives, objectives and the expectations of those whose privacy is invaded. Need to establish there was an expectation of seclusion or solitude was objectively reasonable. “<i>Intrusion upon seclusion</i>” arises only for deliberate and significant invasions of personal privacy into matters such as: financial or health records, sexual practices and orientation, employment, diary or private correspondence. There are limitations to this new tort because protection of privacy may give rise to competing claims and no right to privacy is absolute.

Case Name, Citation and Court	PIPEDA Case Summary #2006-351 – Use of personal information collected by Global Positioning System considered Office of the Privacy Commissioner of Canada
Date	18 January 2012
Subject	GPS monitoring of employees in work vehicles
Key facts	<ul style="list-style-type: none"> • Employer installed GPS in work vehicles and collected personal information about employees while on the job without consent. • According to employer, GPS would be used to locate, dispatch and route employees to job sites, improving efficiency and eliminating wasted idle time. • Start and stop times of the vehicle and its location would be used in capacity planning, productivity analysis and performance management.
Key points	<ul style="list-style-type: none"> • OPC cautioned organizations about “<i>function creep</i>” and the negative effects of technology on privacy. • Use of GPS for safety purposes and asset management was accepted, loss of privacy was proportionate to the benefit gained. • GPS, in this particular instance, was not particularly privacy-invasive. • GPS data would only be used for performance management when it involved investigating a complaint from a member of the public; internal investigations; and addressing productivity issues. • OPC recommended that employers have a clear policy.

Case Name, Citation and Court	R v. Cole, 2012 SCC 53 Supreme Court of Canada
Date	19 October 2012
Subject	Reasonable expectation of privacy of an employee when using a work laptop
Key facts	<ul style="list-style-type: none"> • Accused teacher's work laptop contained sexually explicit nude images of grade 10 student on hard drive. • School board handed the laptop computer over to the police and accused was charged with possession of child pornography. • Evidence from the laptop was excluded on the basis that the police infringed on the accused's right against unreasonable search and seizure pursuant to the Charter of Rights and Freedoms.
Key points	<ul style="list-style-type: none"> • This is the leading case on the principle that an employee may reasonably expect privacy with respect to information that is meaningful, intimate and touching on the user's biographical core. • There is an expectation of privacy on a work computer where personal use is permitted or reasonably expected. • Computers used for personal purposes contain details of a person's financial, medical and personal situations. • This notwithstanding that the school board policy explicitly states nothing stored on the laptop should be expected to be private. • Third-party consent does not apply and an employer does not have the authority to waive the employee's privacy interest under the <i>Charter</i>.

Case Name, Citation and Court	Schindler Elevator Corp., Re, 2012 BCIPC 25, 2012 CarswellBC 4283 British Columbia Office of Commissioner of Information and Privacy (BC OIPC)
Date	19 December 2012
Subject	GPS technology used to track vehicles for safety purposes
Key facts	<ul style="list-style-type: none"> • Employer used GPS technology to track vehicles, producing “exception reports” that record speeding; idling; harsh braking; sharp acceleration etc. • Employer assured employees GPS tracking data in vehicles would not be routinely or continuously monitored for the purpose of managing employee performance with possible disciplinary action.
Key points	<ul style="list-style-type: none"> • Important that GPS information was recorded and stored, and may only be used when there is an investigation into an employee’s conduct. • GPS tracking was accepted as an effective approach and the only apparent alternative; self-reporting, was inaccurate and incomplete. • BC OIPC recommended employer should revise GPS policy to comprehensively set out purposes for information collected and serve as a single source of notice to employees.

Case Name, Citation and Court	Kone Inc., Re 2013 CarswellBC 3946, [2013] BCIPCD No. 23 British Columbia Office of Commissioner of Information and Privacy (BC OIPC)
Date	28 August 2013
Subject	GPS monitoring on cellular phones of employees acceptable
Key facts	<ul style="list-style-type: none"> • Employer used GPS enabled cellular phones for its elevator service mechanic employees, in part for employee management purposes. • There was no evidence that employer was using personal information of employee for purposes other than to manage employment relationship.
Key points	<ul style="list-style-type: none"> • GPS information collected from a phone is more sensitive than GPS information collected from a vehicle, because of the increased accuracy or precision of information collected. • Constant or recurring surveillance related to productivity has generally been rejected. • BC OIPC found that employer satisfied obligations under Personal Information Protection Act and notified employees before collecting GPS information through PowerPoint presentations. • BC OIPC recommended that employer create a specific policy for the phones that sets out the purpose for which GPS information may be collected, used or disclosed.

Case Name, Citation and Court	R v. Mills, 2013 CarswellNL 431 Newfoundland and Labrador Provincial Court
Date	19 November 2013
Subject	Email messages and Facebook Messenger messages considered private communications
Key facts	<ul style="list-style-type: none"> • Police officer created a fake Facebook and email account posing as 14-year-old girl and anyone who contacted account seeking to add the fake profile was subject to surveillance. • Accused contacted the fake profile and the officer used a computer screenshot program that captures video display and audio output to capture communications between accused and fake 14-year-old girl. • This was a breach of accused's Charter of Rights and Freedoms right to be free of unreasonable search.
Key points	<ul style="list-style-type: none"> • The interception of private communications requires consent or authorization under the Criminal Code. • Emails and Facebook Messenger messages between the accused and the fake 14-year-old girl profile are considered private communications. • Actions of police troubling, court considers the impact of "<i>warrantless surveillance</i>". • Police officer should have obtained judicial authorization for the chat and email communications and a general warrant for the Facebook page and photographs

Case Name, Citation and Court	Toronto (City) v. Toronto Professional Firefighters Association, Local 3888, 2014 CanLII 76886 (ON LA) Ontario Arbitration
Date	14 October 2014
Subject	Termination of employee based on off-duty conduct on Twitter
Key facts	<ul style="list-style-type: none"> • Toronto Fire Services (TFS) released diversity and inclusivity initiative with intention to recruit more women into firefighting. • Employee tweeted potentially sexually derogatory comments about women. • Employee thought his tweets were private but they were in fact public. • Employer relied on three tweets to terminate employee for cause and termination was not upheld, employee reinstated.
Key points	<ul style="list-style-type: none"> • Employer was found not to have established just cause for termination. • Two of the three tweets were not found to be offensive or contrary to the employer's policies or the Human Rights Code. • The test is two-fold: (1) decide whether employee's tweets amount to misconduct or breach of employer's policies; (2) determine whether the misconduct warrants discipline or discharge. • Tweets were not directed to anyone in the workplace and appeared to be an isolated incident

Case Name, Citation and Court	SGEU and Unifor, Local 481 (Admissibility), Re, 2015 CarswellOnt 278 Saskatchewan Arbitration
Date	16 May 2015
Subject	Employees' reasonable expectation of privacy when using employer email system
Key facts	<ul style="list-style-type: none"> • Employer's IT policy makes it clear that employees have no expectation of privacy when using the SGEU system. • Emails between employee and his wife were not admissible in arbitration even though they were found on SGEU's email system and SGEU was justified in searching the employee's email.
Key points	<ul style="list-style-type: none"> • IT policy does not completely extinguish an expectation to privacy. • Even a legitimate need to investigate does not give employer carte blanche to conduct a particularly invasive search. • Degree of intrusion is heightened because the emails are between the employee and his wife. • It does not mean an employer never has the right to examine an employee's personal email found on employer's server. • Employer should give notice to employee and the search must be reasonable in the circumstances. • Search of personal emails should not be conducted if reasonable alternatives to acquire information exist.

Case Name, Citation and Court	<i>Video surveillance of employees vs. right to privacy – a delicate balance, Commissioner's Findings Privacy Act</i> Office of the Privacy Commissioner of Canada (OIPC)
Date	10 December 2015
Subject	Video monitoring of employees at work
Key facts	<ul style="list-style-type: none"> • Complaint against the Canada Border Services Agency (CBSA) alleging the use of video surveillance to monitor employee conduct and performance at a border crossing contravened the Privacy Act. • CBSA cited safety and security related reasons for using video monitoring. • OIPC was satisfied CBSA's rationale for collecting employee personal information and its policy met the standard under the Privacy Act.
Key points	<ul style="list-style-type: none"> • Modern video equipment has incredible capacity to capture information and raises serious concerns regarding the impact this technology can have on the privacy of Canadians • CBSA is a law enforcement agency and the cameras are located where employees would reasonably expect to be observed by members of the public, managers and colleagues • CBSA's rationale for using video recordings of employees to formally investigate allegations of serious misconduct was accepted

Case Name, Citation and Court	ATU, Local 113 v. Toronto Transit Commission, 2017 ONSC 2078 Ontario Superior Court of Justice
Date	3 April 2017
Subject	Random drug and alcohol testing policy for public safety reasons
Key facts	<ul style="list-style-type: none"> • Union applied for interlocutory injunction restraining TTC from implementing random drug and alcohol testing of employees. • Injunction not granted and court was satisfied testing would increase public safety by detecting and deterring drug and alcohol use too close to working hours.
Key points	<ul style="list-style-type: none"> • Since the workplace is “<i>literally the City of Toronto and as a result all the people who move about in the city, whether or not they are passengers on the TTC, have an interest in the TTC safely taking its passengers from one place to another</i>”. • The public interest in this case was the safety of everyone in the city of Toronto weighed against the privacy interests of the individual employees. • If the unionized employees are successful in arbitration, they can be compensated with damages for an invasion of their reasonable expectation of privacy.

Summary of existing legislation

Canada has both public sector and private sector data protection legislation. It is important to note that in Canada, employment law is a provincial jurisdiction, with the result that each of the 10 provinces and the three territories have the authority to pass their own employment legislation and privacy legislation. The federal legislation will govern federally-regulated employers including airlines, telecommunication companies, interprovincial and international railways, interprovincial and international trucking and banks. A number of provinces further have specific legislation protecting personal health information and providing patients and other individuals a right to access their own personal health information. These statutes are generally administered by a governmental information and privacy commissioner.

Private Sector Personal Information Protection

The federal Personal Information Protection and Electronic Documents Act (**PIPEDA**) governs the protection of personal information in trade and commercial activities in every province and territory, with the exception of the provinces of Quebec, Alberta and British Columbia which have each passed their own substantially similar legislation. These provinces each have a privacy commissioner which issues rulings under the legislation. PIPEDA incorporates the Canadian Standards Association Model Code for the Protection of Personal Information and is based on the principles set out in the OECD Guidelines.

PIPEDA governs the collection, use, retention, disclosure and access to personal information by federally-regulated employers *qua* employers, as well as non-federally regulated organizations in all but the three provinces listed above in the course of their commercial activities (but not as employers).

PIPEDA incorporates the following 10 principles:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

It applies to “*personal information*”, which is broadly defined to include “*information about an identifiable individual*”. Complaints under PIPEDA are directed to the Office of the Privacy Commissioner of Canada.

The provinces of British Columbia and Alberta have passed a Personal Information Protection Act, both of which are very similar to PIPEDA, although allowing more leeway to provincially-regulated employers in those two provinces with respect to “*employee personal information*”. This is defined as information related to the employment relationship about an identifiable individual which is collected, used or disclosed solely “*for the purposes reasonably required to establish, manage or terminate an employment relationship*”. Both Personal Information Protection Acts allow an employer in those provinces to collect, use and disclose employee personal information without consent upon notice to employees. Generally, business contact information and work product are excluded from the definition of employee personal information, although GPS information has been considered to be personal information rather than work product information.

The province of Quebec, through the Act respecting the protection of personal information in the private sector (the **Private Sector Act**) defines personal information as “*any information which relates to a natural person and allows that person to be identified*”. The Private Sector Act governs collection, use, disclosure and confidentiality of personal information and includes rights of access and rectification.

The Civil Code of Quebec further establishes the following principles. Every person who establishes a file on another person must have a serious and legitimate reason for doing so, the individual concerned has the right of access to the information contained in the file, and the individual establishing the file must respect certain rules as to collection, storage, use and communication of the information.

Public Sector Personal Information Protection

The federal government and most of the provincial governments also have their own freedom of information and protection of privacy legislation, administered by an information and privacy commissioner.

The Constitution Act, 1982

The Constitution of Canada includes the Canadian Charter of Rights and Freedoms. One of the enumerated fundamental constitutionally protected rights is the right to be secure against unreasonable search or seizure. The Charter applies to governmental activities, with the result that unreasonable searches by those carrying out investigations on behalf of the government, such as the police and border security may be challenged.

The Criminal Code

Criminal law in Canada is federal, with the result that every province and territory is governed by the Criminal Code of Canada. It is a criminal offence to intercept private communications. Specifically, the Criminal Code states that it is a criminal offence to wilfully intercept a private communication by means of any electro-magnetic, acoustic, mechanical or other device. This does not apply where the person has the consent, express or implied, of the originator of the private communication or of the person intended by the originator to receive it.

It is not an offence for a person, in possession or control of a computer system to intercept a private communication originating from, directed to or transmitting through that computer system if the interception is reasonably necessary for managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data or the interception is reasonably necessary to protect the computer system in certain circumstances.

Future legislation which may have an impact on employee monitoring

We are not aware of any impending legislation that may impact on employee IT monitoring.

Australia

Australia

Commentary on existing case law

There is limited case law relating to employee IT monitoring. This is likely due to there only being laws regulating such monitoring in New South Wales (NSW) and the Australian Capital Territory (ACT). The surveillance laws in the remainder of Australia do not specifically deal with monitoring of information technology in the workplace.

Further, the privacy laws have broad exemptions from the Australian Privacy Principles in relation to the use of "*employee records*" for a use related to an employment relationship. While this exemption will not cover all information relating to employees, it will generally cover, for example, records created as a result of employee IT monitoring. The employee records exemption would also likely cover the subsequent use of such records for disciplinary or performance related purposes.

The employee records exemption would not cover, however, use for a purpose unrelated to the employment relationship. This means it may not cover the employer providing IT monitoring records to a government authority undertaking an investigation into fraudulent activities by the employee. It would also not cover records created as a result of a third party to the employment relationship conducting the monitoring. While there are limitations to the employee records exemption, it is sufficiently broad that employees may well have limited expectations around their privacy rights relating to monitoring. That employees have limited expectations around their rights to privacy seems confirmed by the limited number of cases in which employees allege breach of the privacy laws by their employer.

There are a greater number of cases relating to employee use of social media. This is likely because disciplinary actions arising from social media use are more open to challenge on the basis that the social media use is not sufficiently related to the employment. That is, that the social media use is either not conducted during work hours or is otherwise not relevant to the employer's interests.

In the cases in which it has been found that it is not related to the employer's interests, the relevant court or tribunal has generally found that any dismissal resulting from the social media use is not fair. This can be contrasted with disciplinary action arising from information gathered as a result of employee IT monitoring. If such information clearly demonstrates, for example, fraud on the employer, disciplinary action is not likely to be successfully challenged on the basis that the fraud is not related to the employer's interests.

Trends that can be identified

Given the scarcity of cases relating to employee IT surveillance, and that no further legislation is to our knowledge impending in this area, it is difficult to identify any definite trends.

It is apparent that Courts and tribunals are prepared to exclude or not rely on evidence gathered in breach of a law or as a result of surveillance that is, in the court's view, an invasion of an employee's privacy. This is consistent with Federal, State and Territory legislation relating to the admissibility of evidence. It may be that employees (and their representatives) will become generally more aware in the future of the limits of the employee records exemption. Should awareness increase, we may see more information excluded on the basis that:

- the information has arisen as a result of employee IT surveillance or monitoring;
- the employer (or person conducting that surveillance or monitoring) did not comply with privacy laws when conducting the surveillance or monitoring; and/or
- the information:
 - was not an employee record; or
 - was not used in connection with a relevant employment relationship.

Existing case law

List of cases

1. *Ruiz v. BHP (AWI) Pty Ltd* [1996] 71 IR 332 (page 200)
2. *C v. Commonwealth Agency* [2005] PrivCmrA 3 (page 201)
3. *Ponzio v. Multiplex Limited* [2005] FCA 1410 (page 202)
4. *Eduard Christiaan Sent and Sandi Porter v. Primelife Corporation Ltd* [2006] VSC 445 (page 203)
5. *Department of Education and Training v. PN (GD)* [2006] NSWADTAP 66 (page 204)
6. *Lever v. Australian Nuclear Science and Technology Organisation* [2007] FCA 1251 (page 205)
7. *Glenn Gervasoni v. Rand Transport* (1986) Pty Ltd [2009] FWA 1269 (page 206)
8. *Fitzgerald v. Dianna Smith t/as Escape Hair Design* [2010] FWA 7358 (page 207)
9. *Richard O'Connor v. Outdoor Creations Pty Ltd* [2011] FWA 3081 (page 208)
10. *Mr Damian O'Keefe v. Williams Muir's Pty Limited T/A troy Williams The Good Guys* [2011] FWA 5311 (page 209)
11. *Stutsel v. Linfox Australia Pty Ltd* [2011] FWA 8444 and *Linfox Australia Pty Ltd v. Stusel* [2012] 217 IR 52 (page 210)
12. *Carolyn Flanagan, Christopher Hogan and Kristian Pitches v. Thalas Australia Limited T/A Thales Australia* [2012] FWA 6291 (page 211)
13. *Rosa Diehm v. Toll Transport Pty Ltd T/A Toll Customised Solutions* [2012] FWA 8818 (page 212)
14. *Bradford Pedley v. IPMS Pty Ltd T/A peckvonhartel* [2013] FWC 4282 (page 213)
15. *Corrective Services NSW v. Danwer* [2013] NSWIRComm 61 (page 214)
16. *Little v. Credit Corp Group Limited t/as Credit Corp Group* [2013] FWC 9642 (page 215)
17. *Shaun Kinnane v. DP World Brisbane Pty Limited* [2014] FWC 4541 (page 216)
18. *Jo v. ComCare* [2016] AIRmr 64 (page 217)
19. *Renton v. Bendigo Health Care Group* [2016] FWC 9089 (page 218)
20. *S v. LED Technologies P/L* [2017] FWC 1966 (page 219)

Case Name, Citation and Court	Ruiz v. BHP (AWI) Pty Ltd (1996) 71 IR 332 Industrial Relations Court of Australia
Date	14 February 1996
Subject	Employee dismissed for workers compensation fraud
Key facts	<ul style="list-style-type: none"> An employer arranged for private investigators to conduct surveillance of an employee's home for a number of days, as it did not believe the employee's workers compensation claim was genuine.
Key points	<ul style="list-style-type: none"> It was held that employee did not engage in fraud or dishonesty and therefore there was no valid reason for dismissal. The employee was awarded compensation and damages.

Case Name, Citation and Court	C v. Commonwealth Agency [2005] PrivCmrA 3 Australian Privacy Commissioner
Date	1 February 2005
Subject	Disclosure by an Australian Government agency under National Privacy Principles to its legal counsel.
Key facts	<ul style="list-style-type: none"> The complainant and his wife were employees of a Commonwealth government department. The complainant's wife was the applicant in proceedings against the respondent in the Administrative Appeals Tribunal for compensation in relation to a health and safety issue. During proceedings the complainant's wife submitted to the Tribunal that she was not able to afford certain medical expenses. In reply, the respondent obtained information about the complainant's income from its payroll department which it submitted to the Tribunal as evidence of the applicant's financial standing. The disclosure was regulated by the National Privacy Principles. The complainant argued that the respondent was not permitted to disclose his personal information to the respondent's legal counsel in relation to a matter which did not concern the complainant.
Key points	<ul style="list-style-type: none"> The Commissioner was satisfied that whilst the personal information relating to the complainant was an employee record, the act of disclosing it to legal counsel (in relation to proceedings involving the complainant's wife) was not an act which was directly related to the complainant's employment, and as such was subject to the National Privacy Principles and did not fall within the employee record exemption in section 7B(3) of the Act. National Privacy Principle 2 sets out the general principle that an organisation must only use or disclose personal information about an individual for the primary purpose of collection. Use and disclosure for a secondary purpose is not allowed except where such a use or disclosure falls within the exceptions listed in National Privacy Principle 2. The respondent advised that the disclosure of the complainant's personal information was for the purpose of gaining legal advice, and for the preparation of legal proceedings. The respondent advised that it was therefore the subject of legal professional privilege and that the disclosure of the information was permitted under National Privacy Principle 2.1(g) which permits a use or disclosure if it is required or authorised by or under law. The Commissioner formed the view that the disclosure of the complainant's personal information to the respondent's legal counsel was authorised by law, as it was subject to legal professional privilege. Therefore the exception in National Privacy Principle 2.1(g) applied.

Case Name, Citation and Court	Ponzio v. Multiplex Limited [2005] FCA 1410 Federal Court of Australia
Date	5 October 2005
Subject	Admissibility of recorded conversation and interviews
Key facts	<ul style="list-style-type: none"> This decision involved an alleged breach of the Workplace Relations Act coercion provisions. The Building Industry Taskforce alleged that a contractor had been coerced by a principal to enter into an industrial agreement with the CFMEU. A key issue in this matter involved whether conversations recorded by one party on a telephone were admissible.
Key points	<ul style="list-style-type: none"> The Federal Court held that a secretly taped conversation was admissible as evidence as it did not contravene the Surveillance Devices Act 1999 (Vic), as one of the parties to the conversation had intended to tape the conversation. This meant that it did not fall within the definition of "<i>private conversation</i>", which requires "<i>the parties</i>" to the conversation to desire it to be private. Whilst the secret taping could be seen as an invasion of the privacy and as involving underhand tactics, it could not be said to have breached the Surveillance Devices Act 1999 (Vic).

Case Name, Citation and Court	<i>Eduard Christiaan Sent and Sandi Porter v. Primelife Corporation Ltd [2006] VSC 445</i> Supreme Court of Victoria
Date	28 November 2006
Subject	Summary dismissal of CEO and Deputy CEO and whether conduct amounted to serious misconduct
Key facts	<ul style="list-style-type: none"> • This case involved the summary dismissal of the CEO and Deputy CEO of Primelife for videotaping board meetings and tapping employees' telephone calls, amongst other things. • The CEO and Deputy CEO engaged in the following conduct: <ul style="list-style-type: none"> • video surveillance policy not being circulated to employees prior to surveillance being set up • employees not being aware board meetings were being filmed • employees not aware that CEO had access in her office to video surveillance • tapping employees telephones without their consent or knowledge.
Key points	<ul style="list-style-type: none"> • Tapping of employees telephones without their consent was found to be a contravention of the Surveillances Devices Act 1999 (Vic). • It was held that Porter's tapping activities were in serious breach of her obligations and her duty of good faith to Primelife, and as such, constituted serious misconduct.

Case Name, Citation and Court	<i>Department of Education and Training v. PN (GD) [2006] NSWADTAP 66</i> New South Wales Administrative Decisions Tribunal Appeal Panel
Date	6 December 2006
Subject	Disclosure of investigation report about an employee to her next employer by employer constituted breach of Privacy Act
Key facts	<ul style="list-style-type: none"> • The employee was a schoolteacher who made a worker's compensation claim. • The employer conducted an investigation into the factors surrounding the worker's compensation claim and from the investigation reached the conclusion that the employee should be transferred to another school. • The principal of the first school sent a copy of the investigation report about a transferring teacher to the next school principal, after the employee had already transferred to the second school.
Key points	<ul style="list-style-type: none"> • It was held that the disclosure was not about "suitability" for employment as the transfer had already happened and was not subject to assessment of other matters such as the investigation report. The information contained in the report therefore did not fall within the exclusion in s4(3)(f) of the Privacy Act. • This was therefore held to be a breach of privacy of the employee.

Case Name, Citation and Court	Lever v. Australian Nuclear Science and Technology Organisation [2007] FCA 1251 Federal Court of Australia
Date	16 August 2007
Subject	Whether dispute between employer and employee prejudiced employee in his employment.
Key facts	<ul style="list-style-type: none"> • The employee claimed that the employer had engaged in a number of breaches against him. • The relevant alleged breach by the employee is that the employer allegedly undertook direct and intrusive surveillance of him in the course of his employment. • Covert surveillance of the employee was designed to be intimidatory and oppressive of the employee and directed to injure him in his employment.
Key points	<ul style="list-style-type: none"> • The employer alleged that the surveillance of the employee by the company's senior offices, would not have contravened the Workplace Surveillance Act 2005 (NSW), even if that Act had been in force in 2004 and even if a State law applied to the activities of a Commonwealth authority. Nor did such conduct contravene the Privacy Act 1988 (Cth). • The proceedings against the employer were dismissed, as the employee failed to establish <u>any</u> of the alleged breaches by the employer.

Case Name, Citation and Court	<i>Glenn Gervasoni v. Rand Transport (1986) Pty Ltd [2009] FWA 1269</i> Fair Work Commission
Date	2 December 2009
Subject	Termination of employment – harsh, unjust and unreasonable
Key facts	<ul style="list-style-type: none"> • Employee was dismissed for driving his truck, in the course of performing his duties, in an unsafe manner. • The employer was able to determine that the employee was speeding while driving the truck, because of a GPS tracking device which was installed on a trailer the employee was driving. • The tracking device was installed and operating without the employee's consent or knowledge.
Key points	<ul style="list-style-type: none"> • It was held that although the tracking system is capable of reporting the geographical position of the trailer and calculating the speed at which it is moving, this was not the primary purpose of the tracking device. • The primary purpose of the tracking system is to remotely monitor the environment in which cold-stored goods are transported. • For that reason, the employer was not required to notify the employee that it was installed. • Nevertheless, the Tribunal found that the employee was not dismissed for a valid reason.

Case Name, Citation and Court	<i>Fitzgerald v. Dianna Smith t/as Escape Hair Design [2010] FWA 7358</i> Fair Work Australia
Date	24 September 2010
Subject	Hairdresser dismissed for posting a comment on Facebook expressing dissatisfaction of employer.
Key facts	<ul style="list-style-type: none"> Employee was dismissed for unauthorised removal of property, lack of punctuality, unauthorised rescheduling of appointments and public display of dissatisfaction with the employer on Facebook.
Key points	<ul style="list-style-type: none"> Commissioner recognised the seriousness of the employee's Facebook post and the increasing tendency for employees to use social networking sites to display their dissatisfaction with their employer. Fair Work Australia emphasised that in certain circumstances, a Facebook post by an employee may be sufficient to warrant dismissal. However, this depends on whether the post will adversely affect the employer's business. The Commissioner ruled that the dismissal was harsh, unjust and unreasonable as the employer failed to demonstrate that the comment damaged business, notwithstanding that it certainly damaged the employer's trust and confidence in the employee. The employer was ordered to compensate the employee \$2,340.48.

Case Name, Citation and Court	<i>Richard O'Connor v. Outdoor Creations Pty Ltd [2011] FWA 3081</i> Fair Work Australia
Date	24 May 2011
Subject	Excessive social media use in working hours may constitute valid reason for termination
Key facts	<ul style="list-style-type: none"> Employee dismissed for misconduct, being excessive social media use in working hours. This included over 3000 transactions on a chat line during work time (in the last three months).
Key points	<ul style="list-style-type: none"> Commissioner held that excessive use of social media during work hours may constitute a valid reason for the termination of employment. However, there was insufficient material in this case to determine if the employee did use social media excessively during working hours.

Case Name, Citation and Court	<i>Mr Damian O'Keefe v. Williams Muir's Pty Limited T/A troy Williams The Good Guys [2011] FWA 5311</i> Fair Work Australia
Date	11 August 2011
Subject	Employee dismissed for threatening behaviour and out of hours Facebook posting
Key facts	<ul style="list-style-type: none"> • An employee posted threatening and offensive posts on Facebook. • The posts included the employee making harsh and offensive and threatening comments about the payroll department at his workplace.
Key points	<ul style="list-style-type: none"> • It was held that the dismissal of the employee was justified, notwithstanding the fact that the employee had applied the most stringent privacy settings to his Facebook account. • Decision was based upon a number of factors including: <ul style="list-style-type: none"> ○ the extremely offensive nature of the allegations and threats made on Facebook; and ○ the fact that the employee's comments could be seen by his colleagues as they were Facebook friends. • The Commissioner also held that it did not matter that the comments were made on a private (as opposed to a business) computer and that they were posted out of hours.

Case Name, Citation and Court	<i>Stutsel v. Linfox Australia Pty Ltd [2011] FWA 8444 and Linfox Australia Pty Ltd v. Stutsel [2012] 217 IR 52</i>
Date	19 December 2011 and 3 October 2012
Subject	Employee was reinstated following termination for allegedly posting derogatory and harassing comments about managers on his Facebook page.
Key facts	<ul style="list-style-type: none"> • Linfox argued that a sufficient nexus existed between Mr Stutsel's conduct and the workplace because: <ul style="list-style-type: none"> ◦ Mr Stutsel had Facebook friends who were employees of Linfox; ◦ the comments were made in respect of various Linfox managers; and ◦ Mr Stutsel's Facebook profile picture featured a Linfox truck.
Key points	<ul style="list-style-type: none"> • The Commission found the comments to be akin to "<i>a group of friends letting off steam and trying to outdo one another in being outrageous</i>", and while in poor taste, did not amount to serious misconduct. • In finding that Mr Stutsel had been unfairly dismissed and ordering his reinstatement and back pay, the Commissioner gave weight to Linfox's lack of a dedicated social media policy at the time of Mr Stutsel's termination or by the date of the hearing, and that Linfox merely relied on its induction training and relevant handbook to ground its action against Mr Stutsel. • The importance of employee awareness and training was also highlighted. • The decision was upheld on appeal from Linfox.

Case Name, Citation and Court	<i>Carolyn Flanagan, Christopher Hogan and Kristian Pitches v. Thales Australia Limited T/A Thales Australia [2012] FWA 6291</i> Fair Work Commission
Date	7 September 2012
Subject	Summary termination of employment for inappropriate use of company computer and email access
Key facts	<ul style="list-style-type: none"> • Employees dismissed for inappropriate use of emails. • Employees argued that surveillance conducted by employer was not in accordance with Thales' policy and in contravention of Workplace Surveillance Act 2005 (NSW). • Employees alleged that they were notified as soon as practicable that their emails would be monitored, which was inconsistent with Thales' Internet and Email Security Framework.
Key points	<ul style="list-style-type: none"> • The Tribunal accepted that Thales did not comply with its notification obligation under the Thales Internet and Email Security Framework, once the monitoring of the employees' emails commenced. • Thales had an obligation to adhere to its policy and in failing to do so, the employees were prejudiced and their dismissal was unfair. • The Tribunal ordered that the employees be reinstated within 14 days of the days of decision.

Case Name, Citation and Court	Rosa Diehm v. Toll Transport Pty Ltd T/A Toll Customised Solutions [2012] FWA 8818 Fair Work Commission
Date	7 November 2012
Subject	Employee dismissed for making false and misleading statements to the employer
Key facts	<ul style="list-style-type: none"> An employer arranged for covert surveillance to be undertaken of employee, as it did not believe that statements the employee were making in respect to her workers compensation claim were truthful.
Key points	<ul style="list-style-type: none"> The National Union of Workers (NUW) submitted that covert surveillance of an employee “<i>in their private life</i>” should not occur when the conduct is wholly innocuous. NUW argued that employer’s actions constituted a breach of privacy in these circumstances. The employee was found to have been unfairly dismissed, and the employee was awarded compensation.

Case Name, Citation and Court	<i>Bradford Pedley v. IPMS Pty Ltd T/A peckvonhartel [2013] FWC 4282</i> Fair Work Commission
Date	2 July 2013
Subject	How an employee's private use of social media can lead to adverse consequences for their employment
Key facts	<ul style="list-style-type: none"> • Bradford Pedley was a Senior Interior Designer with an architecture and design company, PVH. When he took the job, he told PVH he would continue carrying out private design work in his own time through his own business. PVH did not try to stop him. • Mr Pedford sent a group email to some of his LinkedIn connections which explained that he had his own business, and was looking to expand it and take on more work. • When PVH learnt of this they fired him.
Key points	<ul style="list-style-type: none"> • The Fair Work Commission rejected Mr Pedley's claim that his dismissal was harsh, unjust or unreasonable. It held that the LinkedIn email was a clear attempt to solicit business from PVH's clients for his own business, which breached his obligation to PVH to faithfully promote PVH's interests. This was serious misconduct, and was a valid reason to terminate the employment contract.

Case Name, Citation and Court	Corrective Services NSW v. Danwer [2013] NSWIRComm 61 Industrial Relations Commission of NSW
Date	16 July 2013
Subject	Employee dismissed for out of hours serious misconduct
Key facts	<ul style="list-style-type: none"> The employer conducted undercover surveillance of an employee who was the subject of an investigation, for allegedly exposing himself to a young person.
Key points	<ul style="list-style-type: none"> The magistrate accepted the evidence that was obtained from the undercover surveillance conducted by the employer, of the employee exposing himself at a music centre.

Case Name, Citation and Court	<i>Little v. Credit Corp Group Limited t/as Credit Corp Group [2013] FWC 9642</i> Fair Work Commission
Date	10 December 2013
Subject	Dismissal of employee for Facebook posts valid when post damages the employer's reputation or viability.
Key facts	<ul style="list-style-type: none"> • The employee used his personal Facebook account to criticise a third party organisation with which his employer had professional dealings with. • The employee also made sexually aggressive comments about a new employee on his Facebook account. • The employer dismissed the employee for misuse of social media in breach of the Code of Conduct (Code). The employee was aware of the Code and had received training about it.
Key points	<ul style="list-style-type: none"> • The employee did not deny the allegations, or that the conduct breached the Code, but he alleged that the comments were made in his time outside of work. • The Commission said that there was a valid reason for the employee's dismissal, as his conduct: <ul style="list-style-type: none"> ○ seriously damaged the relationship between him and the employer; ○ damaged the employer's interests; ○ potentially damaged the relationship between him and other employees; ○ was incompatible with his duty as an employee; ○ was inconsistent with the Code; and ○ constituted serious misconduct.

Case Name, Citation and Court	<i>Shaun Kinnane v. DP World Brisbane Pty Limited [2014] FWC 4541</i> Fair Work Commission
Date	9 July 2014
Subject	Employee dismissed for fraud and dishonesty in connection with WorkCover claim
Key facts	<ul style="list-style-type: none"> • An employer had concerns about the legitimacy of an employee's WorkCover workers compensation claim, so it conducted covert surveillance of an employee. • The surveillance showed that the employee was performing work that was said to be inconsistent with his medical restrictions.
Key points	<ul style="list-style-type: none"> • It was held that surveillance of an employee outside of the workplace was unreasonable in the circumstances. • At paragraph [99] of this decision, it was held that in relation to the surveillance, the employee's privacy has been invaded and that this is unjust, unreasonable and contrary to a 'fair go'. • The employment relationship confers no right to spy on an employee. The surveillance was initiated when there was no reasonable suspicion and without notification to the employee. The surveillance invaded his privacy and that of his family and was used to justify a predetermined conclusion of fraud. • It was held the employee did not engage in fraud or dishonesty and therefore there was no valid reason for dismissal.

Case Name, Citation and Court	<i>Jo v. ComCare [2016] AIRmr 64</i> Australian Privacy Commissioner
Date	21 September 2016
Subject	Breach of Privacy Act by Comcare for disclosing an employee's workplace injuries at current employer to his former employer and an insurance company.
Key facts	<ul style="list-style-type: none"> • Employee lodged various WorkCover claims against the Department of Defence (Defence), which were referred to Comcare as the authorised insurer. • The employee had previously worked for Department of Human Services (DHS) and in early 2014 also lodged a WorkCover claim with Comcare regarding an injury sustained in 2009 whilst an employee of DHS. Comcare accepted the DHS claim in April 2014, and subsequently closed the DHS claim in September 2014. • In February 2016, the employee received an email from Comcare advising that a new pilot program would change the way his current WorkCover claim with DHS would be managed. Comcare also emailed an excel spreadsheet with the employee's personal information to DHS and the insurer Allianz (which was acting as a contracted service provider to Comcare). • The spreadsheet disclosed the employee's name, contact details, injury dates and WorkCover claims history to DHS and Allianz even though the employee no longer worked with DHS and did not have an active WorkCover claim with DHS for Allianz. • The employee lodged a complaint against Comcare with the Office of the Australian Information Commissioner under the Privacy Act 1998 (Cth) alleging that Comcare had disclosed details of his WorkCover claims history with his current employer, Department of Defence to his previous employer, DHS.
Key points	<ul style="list-style-type: none"> • Comcare was held to have breached the Australian Privacy Principles and interfered with the employee's privacy by improperly disclosing personal information about the employee to DHS and Allianz. It also failed to take reasonable steps to secure the employee's personal information relating to his claims with defence against unauthorised disclosure. • Comcare was required to pay the employee \$3,000 by way of compensation for the loss or damage suffered by the employee by reason of interference with his privacy.

Case Name, Citation and Court	Renton v. Bendigo Health Care Group [2016] FWC 9089 Fair Work Commission
Date	30 December 2016
Subject	Termination for misuse of social media
Key facts	<ul style="list-style-type: none"> • An employee of Bendigo Health Care Group was dismissed for serious misconduct. • The employee “tagged” two of his colleagues in an offensive sexually explicit video post on Facebook. That same day, after posting the video, the employee also left blobs of sorbolene cream and tissues on the desk of the colleague tagged in the video. • The colleague complained about the conduct, and the employer dismissed the employee for serious misconduct.
Key points	<ul style="list-style-type: none"> • The Commissioner held that the employee had: <ul style="list-style-type: none"> ◦ negatively affected the health and safety of colleagues; ◦ engaged in conduct that had the potential to damage the employer’s reputation; and ◦ exposed his colleagues to humiliation and ridicule at work. • Despite this, the Commissioner said the dismissal was disproportionate to his misconduct. This was because of its one-off nature and the lack of previous misconduct. Having found the dismissal of the employee to be harsh, it was therefore found that he was unfairly dismissed.

Case Name, Citation and Court	S v. LED Technologies P/L [2017] FWC 1966 Fair Work Commission
Date	6 April 2017
Subject	Employee dismissed for posting statement on his personal Facebook page.
Key facts	<ul style="list-style-type: none"> • The employee posted on his personal Facebook account saying "<i>I don't have time for people's arrogance. And your not always right! Your position is useless, you don't do anything all day how much of the bosses c*** did you suck to get where you are?</i>" • The post was seen by several of the employees' colleagues before he removed it after five minutes. • The employer dismissed the employee in a sixty second telephone call. The employee was told: "<i>it doesn't matter. You're fired</i>". The employer failed to provide the employee an opportunity to explain his conduct. • The employer mistakenly interpreted that the post was referring to employees of LED Technologies Pty Ltd. • The employee reposted a 'clarification' explaining his original post. He was referring to a hostile employment situation his mother was facing elsewhere.
Key points	<ul style="list-style-type: none"> • The Fair Work Commission found: <ul style="list-style-type: none"> ◦ the Facebook post was "<i>crude and immature</i>"; ◦ the post did not constitute a valid reason for dismissal; ◦ offensive and vulgar language are increasingly part of the common vernacular; ◦ there was no evidence the post was directed at the business or its employees; ◦ no evidence that employee was provided a social media policy; and ◦ there was no sufficient connection to the workplace to justify legitimate action against employee. • Employee was compensated with the difference in his earnings from another role for a period of six months.

Summary of existing legislation

In Australia, there are various pieces of legislation which place different restrictions on employee monitoring. These differ among the various States and Territories. The key acts of legislation are:

- Workplace Surveillance Act 2005 (NSW);
- Workplace Privacy Act 2011 (ACT);
- Invasion of Privacy Act 1971 (Qld);
- Surveillance Devices Act 2007 (NSW);
- Listening Devices Act 1992 (ACT);
- Surveillance Devices Act 1999 (Vic);
- Listening Devices Act 1991 (Tas); and
- Surveillance Devices Act 1998 (WA).

In general, the Acts set out above make it an offence to use:

- listening devices to listen to or record private conversations without the consent of all of the parties to that conversation, except in limited circumstances (such as when a party to the conversation consents to the use of the listening device in order to protect their lawful interests);
- optical surveillance devices (such as CCTV) to record a private activity, except in limited circumstances (such as when a party to the activity consents to the use of the surveillance device in order to protect their lawful interests); or
- tracking devices to determine the geographical location of a person without that person's permission.

'Private' activities or conversations are generally defined to mean conversations or activities that a person involved would not reasonably have expected would be overheard or seen.

More detailed summaries of the Workplace Surveillance Act 2005 (NSW) (**NSW Act**) and the Workplace Privacy Act 2011 (ACT) (**ACT Act**) (collectively, the **Acts**) are set out below. The summaries have particularly focused on the Acts as, of the various pieces of legislation listed above, the Acts are the most:

- restrictive;
- relevant to workplace monitoring; and
- relevant to monitoring of information technology.

Workplace Surveillance Act 2005 (NSW) and Workplace Privacy Act 2011 (ACT)

The Acts principally regulate camera, computer and tracking surveillance.

Camera surveillance (known as surveillance using an optical surveillance device under the ACT Act) is surveillance by means of:

- a camera that monitors or records visual images of activities on a premises or in any other place under the NSW Act; or
- a device capable of being used to record visually or observe an activity under the ACT Act, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

Computer surveillance (known as surveillance using a data device under the ACT Act) is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer. Under the NSW Act, the Parliament has clarified that this includes the sending and receipt of emails and the accessing of internet websites and under the ACT Act, Parliament has clarified that computer surveillance does not include surveillance by an optical surveillance device.

Tracking surveillance (known as surveillance using a tracking device under the ACT Act) is surveillance by means of:

- an electronic surveillance device, the primary purpose of which is to monitor or record geographical location or movement (such as a Global Positioning System tracking device) under the NSW Act; or
- an electronic device capable of being used to work out or monitor the location of a person or an object, or the status of an object (for example, GPS, biometrics or radio frequency identification) under the ACT Act.

Subject to what we say below, employers (which, in the ACT, includes any related body corporate of the person who actually engages the worker) may conduct the above types of surveillance in respect of:

- "employees" (including employees of the employer's related corporations) under the NSW Act; and
- "workers" under the ACT Act.

Subject to some exceptions and to meeting certain notification requirements:

- in NSW, surveillance of an employee may only be conducted when the employee is 'at work' for their employer. An employee will be "at work" when the employee is:
 - at a "workplace" of the employer, whether or not the employee is actually performing work at the time. Workplace is defined to mean "*premises, or any other place, where employees work, or any part of such premises or place*"; or
 - at any other place while performing work for the employer; and
- in the ACT, surveillance of a worker may only be conducted by an employer "*in a workplace*". A workplace is defined by the ACT Act to mean a "*place where work is, has been, or is to be, carried out by or for someone conducting a business or undertaking*".

The Acts set out specific notification and other requirements that must be satisfied before surveillance of employees/workers can be lawfully conducted at work/at the workplace. Where these requirements are not met, the surveillance is tantamount to "*covert surveillance*". Covert surveillance is an offence unless it is authorised by a covert surveillance authority issued by a magistrate. Covert surveillance authorities are only issued for the purpose of establishing whether one or more employees/workers are involved in unlawful activity at work/in the

workplace.

Except in limited circumstances (including where a covert surveillance authority has been obtained), before an employer can conduct surveillance under either Act, it must satisfy certain notification requirements. In particular, an employer must give written notice (email is sufficient at least in NSW and policy is sufficient at least in the ACT) to an employee/worker before conducting any surveillance and that notice must specify:

- in both NSW and the ACT:
 - the kind of surveillance to be carried out or surveillance device to be used;
 - how the surveillance will be carried out;
 - when the surveillance will start;
 - whether the surveillance will be continuous or intermittent; and
 - whether the surveillance will be for a specific limited period or whether it will be ongoing; and
- in the ACT:
 - who will regularly or ordinarily be the subject of the surveillance;
 - the purpose for which the employer may use and disclose surveillance records of the surveillance; and
 - that the worker may consult with the employer about the conduct of the surveillance. This requires the employer to consult (during the notice period set out below) in good faith about the conduct of surveillance so as to give the worker a genuine opportunity to influence the conduct of the surveillance.

Under both Acts, the written notice must be provided at least 14 days before the surveillance commences (or a lesser agreed period) provided that for a new employee/worker, the notice must be provided to the employee before the employee starts work.

It is not necessary to provide this written notice where camera surveillance of an employee/worker is to be undertaken at a workplace that is not the employee/worker's usual workplace.

In addition to meeting notice requirements, an employer must satisfy the following additional requirements before undertaking the following types of surveillance in both NSW and the ACT:

- Camera surveillance:
 - the cameras used for the surveillance (or casings or other equipment that generally indicates the presence of a camera) must be clearly visible in the place where the surveillance is taking place; and
 - signs notifying people that they may be under camera surveillance must be clearly visible at each entrance to the place.
- Computer surveillance:

- the surveillance must be conducted in accordance with a policy of the employer on computer surveillance; and
- the employee/worker the subject of the computer surveillance must have been notified in advance of that policy in a way that it is reasonable to assume that they were aware of and understood the policy.

The ACT Act requires that the abovementioned policy specifically state:

- how the employer's computer resources (which includes internet access and electronic communication applications) may, and must not, be used;
- what information about the use of the employer's computer resources is logged and who may access the logged information; and
- how the employer may monitor and audit compliance with the policy.
- Tracking surveillance - a clearly visible notice must be placed on the vehicle or thing the subject of the tracking surveillance, indicating that the vehicle or thing is being tracked. The Explanatory Memorandum to the ACT Act indicates that this obligation may extend in some cases to smartphones where GPS data can be used to track location. In NSW, notices on smartphones won't be necessary provided the primary purpose of the smartphone is not to monitor or record the location or movement of the employee.

The Acts prohibit surveillance being carried out by an employer in certain circumstances, even where notice and other requirements are met. These prohibited circumstances are as follows:

- an employer must not carry out surveillance of an employee/worker in:
 - any changing room, toilet facility or shower or other bathing facility; and
 - in addition, under the ACT Act, in any parent or nursing room, prayer room, sick bay, or first aid room;
- an employer must not carry out surveillance of an employee/worker:
 - in NSW using a "*work surveillance device*" (ie a device used for the surveillance of the employee when at work for the employer) when the employee is not at work for the employer (unless the surveillance is computer surveillance of the employee's use of equipment or resources provided at the employer's expense); or
 - in the ACT, if the worker is not in a workplace (except where the employer is conducting computer surveillance of the worker's use of equipment or resources provided by the employer or the employer is conducting surveillance using a tracking device that has a tracking function that cannot be deactivated. Any surveillance records obtained from the tracking device in this circumstance cannot be used or disclosed for any purpose);
- an employer must not prevent, or cause to be prevented, the delivery of an email sent to or by, or access to an internet website by, an employee/worker unless:

- the employer's policy on email and internet access details and permits the prevention and the employer is acting in accordance with it; and
- in circumstances where the delivery of an email is prevented, a notice is given to the employee/worker (via email or otherwise), as soon as practicable, to the effect that delivery of the email has been prevented (Prevented Delivery Notice). An employer, however, is not required to give a Prevented Delivery Notice if delivery of the email was prevented in the belief that, or by the operation of a program intended to prevent the delivery of an email on the basis that:
 - the email was a commercial electronic message within the meaning of the Spam Act 2003 (Cth) (**Spam Act**);
 - the content of the email or any attachment would or might have resulted in an unauthorised interference with, or damage to, the operation of, a computer or computer network operated by the employer or of any program run by or data stored on such a computer or computer network;
 - the email or attachment to the email would reasonably be regarded as threatening, menacing, harassing or offensive; or
 - the employer was not aware, and could not reasonably be expected to be aware, of the identity of the employee or worker who sent the communication, or that the communication was sent by the employee or worker; and
- an employer's policy on email and internet access must not provide for prevention of the delivery of an email, or access to a website, merely because the email was sent by, or on behalf of, an industrial organisation of employees or an officer of such an organisation, or the website or email contains information relating to industrial matters.

Under both Acts, restrictions are imposed on an employer's ability to use and disclose any record of information obtained, recorded, monitored or observed as a consequence of regulated or notified surveillance (**Surveillance Record**).

The employer must not use or disclose a Surveillance Record unless the use or disclosure is:

- for a legitimate purpose related to the employment of employees (in the case of the NSW Act) or workers (in the case of the ACT Act) of the employer, or the legitimate business activities or functions of the employer;
- to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
- for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings; or
- reasonably believed to be necessary to avert an imminent risk/threat of serious violence to persons (specifically death or serious injury under the ACT Act) or of substantial damage to property.

In addition, under the ACT Act, the employer:

- must not use or disclose a Surveillance Record to take adverse action (within the meaning of the Fair Work Act 2009 (Cth)) against a worker unless notice given to the worker about the surveillance states

that the employer may use the surveillance to take adverse action against the worker; and

- must, on the written request of a worker, allow the worker access to Surveillance Records in relation to the worker. If the employer fails to do so, the Surveillance Records cannot be used by the employer in legal proceedings between it and the worker or to take adverse action against the worker. Despite this, an employer may refuse a worker access to Surveillance Records if:
 - the disclosure of those records would be an offence under the ACT Act or otherwise unlawful;
 - a law enforcement body performing a lawful security function asks the employer not to allow access to the information on the basis that allowing access would be likely to cause damage to the security of Australia; or
 - the employer is satisfied on reasonable grounds that:
 - allowing access would have an unreasonable impact on the privacy of other individuals;
 - the request for access is frivolous or vexatious;
 - the information relates to existing or anticipated legal proceedings between the employer and the worker and the information would be accessible during the discovery process of those proceedings;
 - allowing access would reveal the intentions of the employer in relation to negotiations with the worker in a way that would be likely to prejudice the negotiations;
 - not allowing access is required or authorised under a law of the ACT or a law of another jurisdiction;
 - allowing access would be likely to prejudice an investigation of possible unlawful activity; or
 - allowing access would be likely to prejudice:
 - the prevention, detection, investigation, prosecution or punishment of a criminal offence or a breach of a law imposing a penalty or sanction;
 - the enforcement of a law relating to the confiscation of the proceeds of crime;
 - the prevention, detection, investigation or remedying of serious improper conduct; or
 - the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders, by or on behalf of a law enforcement agency.

Importantly, the restrictions on the use of Surveillance Records are independent of the restrictions in relation to the conduct of surveillance. This means that the reason for which surveillance was lawfully conducted may not of itself prevent any Surveillance Record obtained from that surveillance being used for some other purpose, provided that other purpose is permitted by the Acts.

Neither of the Acts expressly state that accessing and reviewing an employee's mobile telephone records constitutes surveillance, however, we suspect this is in part because the Acts may not have kept up with technology. Having said that, accessing and reviewing an employee's mobile telephone records could arguably

constitute:

- computer surveillance:
 - under the NSW Act if:
 - the mobile telephone could be considered a 'computer' – and the technology on some smart phones means that they potentially could be; and
 - software or other equipment is used on the mobile telephone to monitor or record where, and to whom, the calls are placed from the mobile telephone; and
 - under the ACT Act if:
 - the mobile telephone could be considered a 'computer' – and the technology on some smart phones means that they potentially could be; and
 - there is a device or program used on that mobile telephone which is capable of recording or monitoring the input or output of information from the mobile telephone (including a record of when and where calls are made); and/or
 - tracking surveillance under potentially both Acts (but more likely, the ACT Act) if:
 - the mobile telephone records show where the employee was located when the employee made a mobile telephone call;
 - the mobile telephone could be regarded as an 'electronic device' (and the Explanatory Memorandum to the ACT Act suggests that smartphones may be electronic devices); and
 - in the case of the NSW Act only, the 'primary purpose' of the mobile telephone is to monitor or record geographical location or movement.

If a VoIP land-line telephone network makes and receives telephone calls via computer over the internet, the monitoring of an employee's calls over that network (including records in relation to such use) could constitute computer surveillance under both Acts.

Privacy Act 1988

The Privacy Act 1988 regulates how "*personal information*" is handled by Australian Government agencies, medium-to-large businesses, the not-for-profit sector, the credit reporting industry and health service providers. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Specifically, the Privacy Act provides for principles as to how personal information is collected, maintained and accessed. These principles are known as the Australian Privacy Principles (APP). The APP provide for:

- APP 1- the requirement that organisations engage in open and transparent management of personal information, including having a privacy policy that specifies:
 - the kinds of information that the entity collects and holds;

- how the entity collects and holds information;
 - the purposes for which the organisation collects, holds uses and discloses personal information;
 - how an individual can access and correct personal information held by the organisation;
 - how an individual may complain about a breach of the APP by the organisation;
 - whether the entity is likely to disclose personal information overseas; and
 - the countries in which overseas recipients of personal information disclosed by the entity are likely to be based.
- APP 2 - an individual having the option of transacting anonymously with organisations, or using a pseudonym where practicable;
- APPs 3 and 4 - requirements relating to the collection of solicited personal information, and receipt of unsolicited personal information, by organisations, including the requirement that:
 - entities only collect personal information if it is reasonably necessary for one or more of the entity's function;
 - entities only collect personal information from the individual, except if the individual:
 - consents to its collection from elsewhere;
 - the entity is required by law or court order to collect it from elsewhere; or
 - it is impracticable to collect it from the individual.
- APP 5 - entities being required to give notice about the collection of personal information, either before that information is collected or as soon as practicable afterwards;
- APP 6 - how personal information can be used (including that if it is collected for a particular primary purpose it cannot be used for a secondary purpose without the individual's consent, except in limited circumstances) and disclosed;
- APP 7 - requirements relating to the use and disclosure of personal information for the purpose of direct marketing;
- APP 8 - requirements relating to cross-border disclosure of personal information, including taking reasonable steps to ensure cross- border entities to whom the information is revealed comply with the APP in relation to the information; requirements relating to maintaining the quality of personal information;
- APP 9 - requirements relating to the adoption, use and disclosure of government related identifiers;
- APP 10 – requirements that an entity take reasonable steps to ensure the personal information it collects is accurate, up to date and complete, and that it is relevant to any purpose for which it is used or disclosed;
- APP 11 - personal information being kept secure; and

- APPs 12 and 13 - rights for individuals to access and correct their personal information.

Further, organisations that are subject to the Privacy Act must comply with notification requirements, if:

- there has been unauthorised access to or unauthorised disclosure of personal information; and
- access or disclosure would likely result in serious harm to affected individuals.

Notification must be to either or both of the affected individuals and the Office of the Australian Information Commissioner.

Significant penalties can be imposed for failure to comply with the APP's. There is, however, a broad exemption that can apply to "*employee records*", depending upon whether those employee records are of public sector or private sector employees.

Non-public sector organisations are not obliged to comply with the APP when handling personal information if that personal information is:

- an employee record; and
- is being handled for a purpose directly related to a current or former employment relationship between the employer and the relevant employee.

An "*employee record*", means a record of personal information relating to the employment of the employee. It includes health information about an employee and personal information relating to:

- the engagement, training, disciplining, resignation or termination of employment of an employee;
- the terms and conditions of employment of an employee;
- the employee's performance or conduct, hours of employment; salary or wages; personal and emergency contact details;
- the employee's membership of a professional or trade association or trade union membership;
- the employee's recreation, long service, sick, maternity, paternity or other leave; and
- the employee's taxation, banking or superannuation affairs.

Employee records could therefore encompass personal information obtained as a result of employee monitoring (e.g. an email relating to an employee's performance or conduct). If information obtained as a result of employee monitoring did come within the definition of employee records, the employer would not be obliged to comply with the APP in its use of those records, provided the use was related to the employment relationship. For example, the employer would be able to use such records in disciplinary matters without being required to comply with the APP.

Employers would not, however, necessarily be able to assume that all the information they collect that relates to an individual employee would be an employee record. For example, emails that an employee has received from third parties outside the organisation may not necessarily be an employee record. Depending on the

circumstances, the exemption may also not cover the content of many other employee emails. Further, if employee monitoring results in records that are used for a purpose unrelated to the employment relationship (e.g. the employer provides IT monitoring records to a government authority undertaking an investigation into fraudulent activities by the employee), the employer must comply with the APP in relation to those records.

An employer may also use employee records for a purpose related to the employment relationship, but in the course of doing so may supply them to a third party (e.g. the employer may supply the records to a payroll processing provider). That third party must comply with the APP in its handling of the information. Further, if that third party is subject to a data breach, the employer may be required to notify that breach to both the affected individuals and the Office of the Australian Information Commissioner.

Further, personal information about an employee can only come be subject to the employee records exemption if the information relates to a current or former employment relationship between the individual and the organisation handling the information. It will not be subject to the employee records exemption if the information is gathered and handled by a third party. This means that any third party monitoring employees must comply with the APP in the handling of any personal information arising as a result of that monitoring.

Finally, any personal information gathered about prospective employees will not be subject to the employee records exemption. This is because the exemption will only apply in relation to handling of employee record for a purpose directly related to a current or former employment relationship. This means that employers are obliged to comply with the APPs when conducting pre-employment checks, including reviewing a potential employee's social media usage.

Telecommunications (Interception and Access) Act 1979 (Cth)

This Act applies across all States and Territories in Australia, and provides that it is an offence to intercept a communication passing over a telecommunication system. 'Intercept' is defined to mean listening to or recording, by any means, a communication in its passage over that telecommunications system without the knowledge of the person making the communication. There are only limited exceptions to this prohibition, such as if a warrant has been issued.

Evidence Act 1995 (Cth)

The Evidence Act 1995 provides that evidence is not to be admitted if it has been obtained:

- improperly or in contravention of an Australian Law; or
- as a consequence of an impropriety or contravention of an Australian Law.

The evidence can, however, be admitted if the desirability of admitting the evidence outweighs the undesirability of admitting it.

This Act applies in all proceedings in a Federal Court. Similar prohibitions apply in all State and Territory Courts.

Future legislation which may have an impact on employee monitoring

We are not aware of any impending legislation that may impact on employee IT monitoring.

Middle East

UAE

Commentary on existing case law

There is very little publicly available case law in the UAE and no effective or reliable way of searching for it. Furthermore, as the UAE is a civil jurisdiction, there is no binding precedent system. Therefore, even if any cases were to be published in relation to employee monitoring, they could not be used as a reliable means of interpreting how such matters may be judged by a UAE Court in the future.

Trends that can be identified

N/A - see paragraph directly before and directly after.

Existing case law

We have carried out an online search on Westlaw Gulf (the principal online source of case law and legislation in the UAE) for case law related to employee monitoring but this did not yield any results.

Summary of existing legislation

At the present time, there is no specific privacy or data protection legislation in place at a federal level in the UAE, and as such there is nothing that contemplates consent or notification requirements in a similar manner to what is seen in other international frameworks.

Protection of personal data and privacy / confidentiality is provided for by the Constitution of the UAE, which provides that "*freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with law*", and various provisions contained within a number of other laws - some of which apply generally / broadly to prohibit the unauthorized use or disclosure of private information (such as Federal Law 3 of 1987 as amended (the **UAE Penal Code**), Federal Law 5 of 2012 regarding Information Technology Crime Control (the **Cyber Crime Law**) and Federal Law 5 of 1985 regarding Civil Transactions as amended (the **Civil Code**) and others which are more sector specific (such as obligations imposed on communications operators in relation to the subscriber data they hold under the Telecoms Law and related regulatory framework)).

Article 379 of the UAE Penal Code provides that anyone who, by reason of his profession, craft, situation or art is entrusted with a secret and who discloses it in cases other than those permitted by law, who uses it for his own advantage or another person's advantage commits an offence, unless the individual (whether an employee, business partner, customer or patient) to whom the secret pertains has consented to such disclosure or use. Therefore, any use of personal information obtained from employees should only be carried out with the relevant employee's explicit consent to such use, and general principles of confidentiality should be applied.

Under the Penal Code, where an unauthorized disclosure of personal data results in a breach of the Penal Code, and if the UAE Courts find a suspect guilty of disclosing secrets that were entrusted to him "*by reason of his profession, craft, situation or art*" the penalties to be imposed may include a fine of up to UAE Dirhams 20,000 (approximately GBP 3,870) (the fine is determined by the Courts) and an imprisonment for at least one year. More generally, pursuant to Article 378 of the UAE Penal Code, "*a punishment of confinement and fine shall be inflicted on any person who attacks the sanctity of individuals' private or family life*" by committing any of the acts described under Article 378 "other than the legally permitted cases or with the victim's consent."

When ruling on the criminal case, the Criminal Courts would usually transfer a civil claim made by the data subject/employee to the Civil Courts of First Instance for further consideration. The data subject/employee would need to prove the losses he/she has suffered as a direct result of the disclosure of his/her personal data before the Civil Courts in order for damages to be awarded.

Where the unauthorised disclosure of personal data results in a breach of the UAE Cyber Crime Law, if found guilty of an offence, the punishment an offender can receive varies depending on the nature of the crime. Punishments range from temporary detention, a minimum prison sentence of between six months or one year and/or a fine between UAE Dirhams 150,000 (approximately GBP 29,028) and UAE Dirhams 1,000,000 (approximately GBP 193,518). If found guilty of an attempt to commit any of the relevant offences under the UAE Cyber Crime Law, the punishment is half the penalty prescribed for the full crime.

In light of the above, and further because the Middle East as a region has heightened cultural sensitivity about what constitutes personal or private information, it is therefore advisable and prudent that employers ensure that appropriate disclosure and consent mechanisms are used at all times when collecting and subsequently processing data in relation to employee monitoring (this would help mitigate potential liability if, for example, there was an inadvertent data breach and an employee's personal information was disclosed). This need not be

express (although that would be best practice, for example by including them in the employee's employment contract) and can be duly accomplished via consent and notice wording contained in the terms and conditions that either accompany or are included in the employer's HR policies and handbooks. Similarly, these terms and conditions should also contemplate that such information may be shared amongst the employer's affiliates and that consent is also provided in this context. Therefore, an employee's IT audit logs and social media or Dark Web access may be monitored by an employer in the UAE provided the employee has, either directly or indirectly, consented to such monitoring.

Lastly, there are certain free zones in the UAE that do in fact have comprehensive data protection legislation. These include the Dubai International Financial Centre (**DIFC**) and Abu Dhabi Global Markets (**ADGM**). However, these laws apply only to entities licensed and operating within such free zones.

Future legislation which may have an impact on employee monitoring

It is worth noting that privacy and data protection is an area of law where we are anticipating further imminent changes in the UAE in light of recent developments in privacy laws in Qatar, which has just become the first GCC country to have a national level comprehensive privacy law regime. This is because we often see a GCC regional regulatory 'domino effect' – i.e. once one GCC country is the first of its kind to enact a particular framework (which is the case with the Qatar data protection regime), the others are likely to follow suit soon thereafter. We have also been informed during the course of informal conversations with the UAE communications regulatory authority over recent months that such a law is in draft form in the UAE and expected to be enacted in the near future, so this is a particularly fluid area that should be monitored closely moving forward.

Asia Pacific

Executive summary

It is very difficult to generalise in relation to the Asia-Pacific region, given the scope of this report considers only the position in Singapore and India.

It can be seen that **Singapore** has few legal barriers to employee IT monitoring in the workplace with the question of whether monitoring can be carried out or not likely to come down to a contractual agreement between employers and employees. In this respect, it is not uncommon for companies to have signed agreements in place which afford them the right to monitor employee communications on company IT systems.

As will be seen however, while there is a lack of case law in relation to employee monitoring (although it is noted that courts often follow UK common law), there is personal data protection legislation in place. This seeks to balance protection for individuals with the needs of organisations to collect, use and disclose personal data, as is reasonable and appropriate to the circumstances. This legislation sets out when employers may process employee data without consent, for example, where used for evaluative purposes. Further detail is given in the summary of legislation section.

It is noted that there is also a law of confidentiality which covers a wide range of data but that there is no statutory or constitutional right to privacy in Singapore.

By contrast, **India** does recognise a right to privacy under the scope of Article 21 of the Constitution of India, which has been upheld in the context of state actors. This has been held by the Supreme Court to extend to telephone-tapping such that surveillance of employees without obtaining prior consent is likely to come under legal scrutiny. An example given within the case law concerns an employer who sought to extensively install CCTV cameras including in relation to a restroom. The Madras High Court ruled that the restroom camera be removed on the ground that it was the employees' private area.

In addition, there are some primary pieces of legislation in force in India governing employee data protection, in the context of specific information technology legislation, which *inter alia* provide rights for a compensation right in case of negligence by a body corporate handling any sensitive personal data or information in implementing reasonable security practice and procedures.

The legislation also imposes a criminal penalty for any person who secures access to electronic records without consent, such that employee surveillance is only possible with the informed consent of employees.

As will be seen, India is also looking to pass a future Data Protection Bill to apply to both state and non-state actors, following a recommendation of the Supreme Court of India (in a case known as *Puttaswamy*). It is anticipated that this future data protection law in India, if introduced, would have further impact for employers.

Note also some specific legislation in relation to the interception of messages which permits the interception of messages only in the case of direction issued by the designated government officers at central or state level.

India

Commentary on existing case law

- The right to privacy as an enforceable right under Article 21 of the Constitution of India has been upheld in the context of state actors. In decisions relating to the Right to Information Act 2005, the Supreme Court has observed that public sector employers are under a fiduciary obligation to protect the confidential information of their employees and this information is exempt from disclosure in the absence of any compelling public interest.
- In *Justice K.S. Puttaswamy v. Union of India & Ors.*²⁴ (**Puttaswamy**), the Supreme Court of India has recommended the framing of a data protection law that will cover both state and non-state actors. The impact of this decision for employer-employee data protection programs is that there is a necessary requirement for informed, individualised consent of employees to any monitoring or surveillance of their information. The future Data Protection Bill resulting from this judgement is likely to emphasise employees' consent and accountability of employers as the two key factors required for such programs.
- The decision in *Canara Bank*,²⁵ cited in *Puttaswamy*, can also be relied upon to argue that private actors are under an obligation to utilise confidential information placed in their custody only for the purpose for which it was provided and not otherwise. The Supreme Court held that 'privacy attaches to persons and not to places.' Similarly in *People's Union of Civil Liberties v. Union of India*,²⁶ the Supreme Court held that telephone-tapping at home or at work would violate the right to privacy under Article 21 of the Constitution of India. Therefore, any surveillance of employees without obtaining prior consent is bound to come under legal scrutiny.
- The Supreme Court of India has, by virtue of its power under Article 141 of the Constitution of India, from time to time, issued guidelines for the enforcement of fundamental rights in the absence of any legislative framework governing the same, which have been made applicable to the private sector as well e.g. guidelines for prevention of sexual harassment at the workplace.
- The Karnataka High Court's decision relating to taxi aggregators in *Satish N v. State of Karnataka & Ors.*²⁷ emphasises that under the Information Technology Act 2000 and the rules thereunder, the principles of notice, consent, and limitation of purposes for which data may be collected, used and retained, are of utmost importance in judging the validity of any rule or policy which allows the collection of personal information. At the same time, the Delhi High Court's decision in *Karmanya Singh Sareen v. Union of India & Ors.*²⁸ indicates that in the absence of any statutory framework, courts may be hesitant to interfere in privacy policies in private contracts where employees have expressly consented to the company's collection and sharing of their personal information.

²⁴ (2017) 10 SCC 1.

²⁵ District Registrar and Collector, Hyderabad v.. Canara Bank, (2005) 1 SCC 496.

²⁶ AIR 1997 SC 568.

²⁷ (2017) 2 KarLJ 6.

²⁸ (2016) 233 DLT 436 (DB).

Trends that can be identified

There are no specific industry-wide trends that we have come across. However, multi-national companies that have their subsidiaries in India have generally ensured that they have built in an appropriate mechanism, which is in accordance with their global policies and code of conduct, to ensure/facilitate monitoring of employee correspondence and communication. Such steps are taken in order to avoid any unauthorised transmission of confidential data and information pertaining to the company to any third party.

Existing case law

List of cases

1. *People's Union of Civil Liberties v. Union of India & Anr.* AIR 1997 SC 568 (page 243)
2. *Girish Ramchandra Deshpande v. Central Information Commissioner & Ors.* 3 (2013) 1 SCC 212 (page 244)
3. *Raptakos Brett Employees Union v. Deputy Commissioner of Labour & Ors.* W.P. No. 29883 of 2013, Madras HC (page 245)
4. *Karmanya Singh Sareen v. Union of India & Ors.* (2016) 233 DLT 436 (DB) (page 246)
5. *Satish N. and Ors. v. State of Karnataka & Ors.* (2017) 2 KarLJ 6 (page 247)
6. *Justice K.S. Puttaswamy and Anr. v. Union of India & Ors.* (2017) 10 SCC 1 (page 248)

Case Name, Citation and Court	People's Union of Civil Liberties v. Union of India & Anr. [AIR 1997 SC 568] Supreme Court of India
Date	18 December 1996
Subject	Telephone-tapping; right to privacy
Key facts	<ul style="list-style-type: none"> A petition challenged the constitutional validity of Section 5(2) of the Indian Telegraph Act 1885 on grounds that it violated the right to privacy under Article 21 of the Constitution of India.
Key Points	<ul style="list-style-type: none"> The right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. The right to hold a telephone conversation in the privacy of one's home or office without interference can be claimed as a right to privacy. Conversations on the telephone are often of an intimate and confidential character and part of a modern individual's life. A right to privacy would certainly include a telephone conversation in the privacy of one's home or office. The right to freedom of speech and expression is guaranteed under Article 19(1)(a) of the Constitution of India. This freedom means the right to express one's convictions and opinions freely by word or mouth, writing, printing, picture or in any other manner. When a person is talking on the phone, they are exercising their right to freedom of speech and expression. Telephone tapping would breach Article 19(1)(a) of the Constitution of India, unless it comes within the grounds of restrictions under Article 19(2) of the Constitution of India. The court laid down procedural guidelines to permit wire-tapping to government agencies in cases of public emergency or in the interest of public safety.

Case Name, Citation and Court	Girish Ramchandra Deshpande v. Central Information Commissioner and Ors. (2013) 1 SCC 212 Supreme Court of India
Date	3 October 2012
Subject	Employer's obligation to protect employee's personal information
Key facts	<ul style="list-style-type: none"> An application was filed by the petitioner under the Right to Information Act 2005 to the Regional Provident Fund Commissioner (Ministry of Labour, Government of India) seeking details of the respondent's personal matters pertaining to his service career, assets and liabilities, movable and immovable properties.
Key Points	<ul style="list-style-type: none"> The court was in agreement with the Central Information Commissioner and the lower courts that the details called for by the petitioner i.e. copies of all memos issued to the respondent, show-cause notices and orders of censure/punishment, etc. are qualified to be personal information as defined in Section 8(i)(j) of the Right to Information Act 2005. The performance of an employee is primarily a matter between the employer and the employee and normally those aspects are governed by the service rules which fall under the definition of 'personal information', the disclosure of which has no relationship to any public activity or public interest. On the other hand, such disclosure would cause unwarranted invasion of privacy of that individual. Similarly information relating to income tax returns would be personal information, which stands exempted from disclosure under Section 8(i)(j) of the Right to Information Act 2005. The Court cited its earlier decision in <i>CBSE v. Aditya Bandhopadhyay</i> where it has observed as obiter that "<i>if on the request of the employer, an employee furnishes his personal data and information, to be retained in confidence, the employer is expected to hold such personal information in confidence as fiduciary, to be made use of or disclosed only if the employee's conduct or acts are found to be prejudicial to the employer.</i>"²⁹

²⁹ CBSE v.. Aditya Bandhopadhyay, (2011) 8 SCC 497.

Case Name, Citation and Court	Raptakos Brett Employee's Union v. The Deputy Commissioner of Labour and Ors. [W.P. No. 29883 of 2013] Madras High Court
Date	1 December 2014
Subject	Closed Circuit Television (CCTV) camera monitoring of employees
Key facts	<ul style="list-style-type: none"> The employer's management had installed 38 CCTV cameras in the factory, and had proposed installing cameras in the restroom as well. The petitioner contended that the installation of such CCTV cameras violated the workers' right to privacy under Article 21 of the Constitution of India.
Key Points	<ul style="list-style-type: none"> The court directed the removal of CCTV cameras in the restroom on the grounds that it was the employees' private area, wherein, no factory fixtures or raw materials were stored, neither were any production of goods or operations taking place. Hence, the employer's surveillance on this particular channel was not warranted. However, from this judgment, it can be inferred that CCTV camera monitoring will be permissible in public areas, for legitimate purposes. The courts have allowed the use of CCTV's in court complexes³⁰ and educational institutions³¹ for the purpose of monitoring the premises.

³⁰ Pradyuman Bisht v. Union of India & Ors. (2017) SCC Online SC 1136

³¹ Kerala Self Financing Engineering College Managements Association v. Mahatma Gandhi University & Ors. (2015) 4 KLT 652

Case Name, Citation and Court	Karmanya Singh Sareen v. Union of India & Ors. (2016) 233 DLT 436 (DB) Delhi High Court
Date	23 September 2016
Subject	Right to privacy-Protection of interest of 'WhatsApp' users
Key facts	<ul style="list-style-type: none"> WhatsApp proposed to change its privacy policy after acquisition by Facebook to allow sharing of user account information with Facebook and all its group companies to improve its advertisements and product experiences. A writ petition was filed challenging the validity on grounds of right to privacy under Article 21 of the Constitution of India.
Key Points	<ul style="list-style-type: none"> The court stated that the privacy policy was part of a private contract between WhatsApp and its users. The policy explicitly stated that it could be revised at any time and that it was governed by the laws of California. Since the terms of the policy were not traceable to any Indian statute or statutory provisions, the petition was not amenable to writ jurisdiction under Article 226 of the Constitution of India. The court noted that under the privacy policy of WhatsApp, users were given an option to delete their WhatsApp account at any time, in which event the information of the users would be deleted from the servers of WhatsApp. Therefore, it was always open to the existing users of WhatsApp who did not want their information to be shared with Facebook to opt for deletion of their account. The Court directed WhatsApp to remove all information relating to such users and recommended the Central Government to consider measures for bringing the said instant messaging platforms under a statutory regulatory framework. The matter is currently pending before the Supreme Court of India.

Case Name, Citation and Court	Satish N. and Ors. v. State of Karnataka and Ors. 2017 (2) KarLJ 6 Karnataka High Court
Date	10 November 2016
Subject	Right to privacy on technological platforms
Key facts	<ul style="list-style-type: none"> The state government of Karnataka enacted the Karnataka On-Demand Transportation Technology Aggregators Rules 2016 (Aggregator Rules) to regulate Uber, OLA and other technological transport service providers that act as an intermediary between taxi drivers and customers (Aggregators). The Aggregators challenged the constitutional validity of the Aggregator Rules. One of the grounds of challenge was that the Aggregator Rules violated the right to privacy under Article 21 of the Constitution of India.
Key Points	<ul style="list-style-type: none"> The court observed that the right to privacy has to be protected and promoted by the judiciary. If people have disclosed personal information to third parties for a limited purpose, it should not be made available to others or the State without a compelling reason. The court observed that the information required to be recorded under Rule 10(c) of the Aggregator Rules, such as details of the passenger and destination of the journey, may reveal the social, or political relationship, and sexual orientation of a passenger. The court held that Rule 10(c) and Rule 10(v.) of the Aggregator Rules did not provide any safeguard to the passenger against such intrusion of his right of privacy, nor did it prescribe the circumstances under which the licensing authority could demand the stored electronic information. Therefore, they violated the right to privacy under Articles 19 and 21 of the Constitution of India. Any disclosure by a digital or online intermediary has to be in accordance with the Information Technology Act 2000 (IT Act) and the Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules). The court held that the Aggregator Rules were contrary to the IT Act and the SPDI Rules as they did not specify the purpose for which information could be disclosed.

Case Name, Citation and Court	Justice K S Puttaswamy and Anr. v. Union of India and Ors. (2017) 10 SCC 1 Supreme Court of India
Date	24 August 2017
Subject	Right to privacy
Key facts	<ul style="list-style-type: none"> The constitutional validity of the Government's 'Aadhar Card' scheme was challenged (Aadhaar is a twelve digit unique identity number issued to all Indian residents based on their biometric and demographic data). Previously, the courts in <i>MP Sharma and Ors. v.. Satish Chandra, District Magistrate, Delhi and Ors.</i>³² and <i>Kharak Singh v.. State of U.P. and Ors.</i>³³ had held that the right to privacy is not a fundamental right under Article 21 of the Constitution of India. The instant case was referred to a nine judge constitution bench to examine whether right to privacy is a fundamental right.
Key Points	<ul style="list-style-type: none"> The court overruled <i>MP Sharma and Kharak Singh</i> and held that the right to privacy safeguards individual autonomy and choice of living and therefore is part of the right to live with dignity and personal liberty in Article 21 of the Constitution of India. Any invasion of privacy must meet the three-fold requirement of: (i) a law which stipulates a procedure which is fair, just and reasonable; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality, which ensures a rational nexus between the objects and the means adopted to achieve them. Informational privacy is a facet of right to privacy. Dangers to privacy can be from non-state actors as well. Therefore, there has to be a robust data protection regime balancing individual interests with legitimate state interests. Such aims would include protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits.

³² (1954) SCR 1077.

³³ (1964) 1 SCR 332.

Summary of existing legislation

Introduction

India does not have comprehensive legislation on data protection or specific legislation related to employee monitoring. The current legal framework is fragmented into different legislations and judicial decisions regarding the rights and obligations of persons handling and providing personal information.

Constitution of India 1950

- Article 21 of the Constitution of India guarantees the fundamental 'right to life and personal liberty.' In *Puttaswamy* a nine judge bench of the Supreme Court of India upheld the right to privacy as part of the constitutionally protected right under Article 21.
- While fundamental rights in Part III of the Constitution of India are ordinarily enforceable only against State actors, the Supreme Court has recommended the Union Government to formulate a data protection regime safeguarding against dangers to privacy from non-state actors.

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

- Currently these are the primary legislations governing employee data protection.
- Section 43A of the IT Act provides for compensation in case of any negligence by a body corporate handling any sensitive personal data or information (**SPDI**)³⁴ in implementing 'reasonable security practices and procedures'. The definition of these procedures includes privacy policies and software monitoring programs to prevent unauthorised use or access. Section 72A of the IT Act prescribes imprisonment or fines as a penalty for disclosure of information in breach of contract.
- Section 72 of the IT Act prescribes criminal penalty for any person who secures access to electronic records without consent. Therefore any kind of employee surveillance will only be possible with the informed consent of employees.
- The SPDI Rules mandate that a body corporate handling such information should mandatorily provide a

³⁴ Rule 3, SPDI Rules 2011 defines SPDI of a person as 'means such personal information which consists of information relating to :-

- (i) Password;
- (ii) Financial information such as Bank account or credit card or debit card or other payment instrument details;
- (iii) Physical, physiological and mental health condition;
- (iv) Sexual orientation;
- (v) Medical records and history;
- (vi) Biometric information;
- (vii) Any detail relating to the above clauses as provided to body corporate for providing services; and
- (viii) Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

Provided that, any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these Rules.

policy for privacy and disclosure of information, make it known to the providers of the same, use it only for a lawful purpose and not store it longer than is necessary for such purpose.³⁵ The SPDI Rules also give the information provider the option to withdraw consent for provision of such information.³⁶ Employers may disclose or transfer SPDI to third parties within India and abroad only with the consent of the concerned employee.³⁷

- The employer is required to implement security procedures in line with ISO standards.³⁸
- Current legislation draws a dichotomy between personal information or SPDI and other kinds of information. Access to employee devices may be permissible, so far it is only to monitor workplace-related communication and not intercept any other kind of information. The employer may therefore require as a pre-emptive measure that workplace devices will not be used for communication of personal information.
- However, there is a grey area in the legislation as it does not address inadvertent discovery of SPDI in the course of employee surveillance or as a result of employee negligence. Nor does it address the privacy-related implications of a general employee monitoring program. It is therefore advisable to obtain written consent of employees prior to using any monitoring software to avoid legal consequences of such situations.

Indian Telegraph Act 1885 read with the Indian Telegraph Rules 1951

- Rule 419A of the Indian Telegraph Rules 1951 allows interception of messages only in case of direction issued by the designated government officers at the Centre or State level. Hence any unauthorised surveillance of telephone or mobile phone conversations or messages may amount to a statutory violation in addition to violating the right to privacy.
- However messages 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.³⁹

Right to Information Act 2005

- Section 8(i)(j) of the Right to Information Act 2005 exempts disclosure of personal information which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority is satisfied that the larger public interest justifies the disclosure of such information.

³⁵ Rule 4, SPDI Rules 2011.

³⁶ Rule 5(7), SPDI Rules 2011.

³⁷ Rule 7, SPDI Rules 2011.

³⁸ Rule 8 . SPDI Rules 2011.

³⁹ State v. Navjot Sandhu, (2005) 11 SCC 600; R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471.

Future legislation which may have an impact on employee monitoring

Data (Privacy and Protection) Bill 2017 (**Data Protection Bill**)

- The Data Protection Bill was introduced in the Lok Sabha (Lower House of the Parliament) in July 2017. The Data Protection Bill provides for collection, storage, transfer (including cross-border transfer) and disclosure of personal information, subject to prior express and informed consent from the concerned person for the purpose of performance of contract or the employer's/data collector's legitimate interests.
- However, the Data Protection Bill expressly bars surveillance by private body corporates. It can only be carried out by public servants or persons authorised by the Central Government, for purposes of national security, maintenance of public order, etc.. The exact demarcation between collection of personal information and surveillance is unclear - the Data Protection Bill implies that while the employer may solicit personal information from the employee for the purpose of maintenance of records, recruitment, etc. any sort of monitoring of employees' data will not be permissible.
- The Data Protection Bill includes 'racial or ethnic origins' and 'political or religious views' in the definition of SPDI, and bars any sort of profiling or harassment based on personal data, providing for compensation to victims of the same. This has legal implications for any employer-installed software or AI programs seeking to profile employees.
- The Bill proposes constitution of 'Data Privacy and Protection Authority' for enforcement and adjudication of disputes.
- The Data Protection Bill also provides for the overriding effect over the IT Act.
- The present status of the Data Protection Bill in light of *Puttaswamy* and the formation of the Committee of Experts is unclear. It may be used as a guideline for future legislation.

White Paper on Data Protection in India 2017 (**White Paper**)

- After the Supreme Court's Recommendation in *Puttaswamy*, the Central Government set up a Committee of Experts (**Committee**) under the chairmanship of the retired Supreme Court judge Justice B.N. Srikrishna, to draft a data protection bill. The Committee published the 'White Paper' outlining proposals for the bill and inviting public comments on the same.
- The Committee has proposed that any future law on data protection should extend not only to entities processing data within India but also companies and establishments outside of India which are offering goods or services to Indian residents or conducting business in India.
- The Committee has emphasized the importance of consent from the information provider prior to the obtaining of any personal data i.e. data that may cause identification of the individual. In order for the consent to be valid, it should be freely given, informed and specific to the processing of personal data by way of a well-designed notice. However the standard of consent may vary depending on the specific transaction.

- The White Paper has also examined issues relating to data localisation, cross-border flow of data, and the need for restrictions to prevent processing of data for illegitimate purposes, and to expand the definition of SPDI to include socio-economic signifiers that can lead to discrimination (especially given that caste discrimination is endemic in India).
- The White Paper proposes creation of a Data Protection Authority for enforcement, monitoring, setting of standards and awareness generation

Singapore

Commentary on existing case law

In Singapore there are few legal barriers to employee IT monitoring in the workplace.

Ultimately the question of whether monitoring can be carried out will likely come down to contractual agreement between the employer and its employees. In Singapore, it is not uncommon for companies to have signed agreements in place which afford them the right to monitor their employees' communications on company IT systems, as a protective measure.

Trends that can be identified

Security

- After collecting personal data, employers have a duty to safeguard it. Reasonable security arrangements must be made to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to the personal data.
- Usage of closed-circuit television cameras (**CCTVs**) in work premises is common and acceptable. Whether or not employers have to notify their employees when CCTV is deployed depends on the purpose for which the CCTV footage is being collected, used or disclosed.

Bring Your Own Device

- Several companies are adopting the bring your own device (**BYOD**) strategy. While having some commercial advantages, BYOD makes it more difficult for employers to monitor their employee's behavior or ensure that confidential information is not leaked.

Existing case law

While there is no Singapore case law in relation to employee IT monitoring in the workplace, as a common law jurisdiction, UK case law is often relied upon by the Singapore courts when there is no applicable Singapore case law. In this regard, please refer to the UK case summaries provided.

Summary of existing legislation

Personal Data Protection Act 2012 (the PDPA)

- The PDPA was introduced to recognise and balance the right of individuals to protect their personal data and the needs of organisations to collect, use and disclose personal data as would be reasonable and appropriate in the circumstances.
- Collection, use and disclosure of personal data requires the consent of the person whose personal data is being collected and used.
- Personal data is defined very generally and could include the information in an employee's personal email account.
- The PDPA allows employers to collect, use and disclose personal data without obtaining the employee's consent or notifying them where it is necessary for evaluative purposes. Evaluative purposes include the determination of the suitability or eligibility of an individual to whom the data relate for employment, continuance in employment or promotion.
- In relation to managing and terminating an employment relationship, employers are permitted to collect personal data of employees without their consent if the collection is reasonable for their purpose. The use or disclosure of such personal data is also allowed if it is consistent with the purpose of the collection. However, employers must still notify their employees of the purpose of such collection, use or disclosure.
- Employers may need to transfer their employees' personal data out of Singapore for various reasons. Under the PDPA, an organisation which transfers personal data out of Singapore must take appropriate steps to: (i) ensure that it complies with the obligations under the PDPA; and (ii) ensure that the recipient is bound by legally enforceable obligations to provide the personal data a standard of protection that is comparable to the PDPA.
- When an employee leaves the company, the employer should cease to retain all documents containing the ex-employee's personal data or remove the means by which the personal data can be associated with the ex-employee, unless there is a clearly defined purpose for retaining it or if it is necessary for legal or business purposes.

There is a law of confidentiality which covers a wide range of data . However, neither the PDPA nor the law of confidentiality expressly deals with monitoring by an employer of an employee's emails on its IT systems.

There is also no statutory / constitutional right to privacy in Singapore.

Future legislation which may have an impact on employee monitoring

As the PDPA is relatively new, we are not aware of any plans for future legislation in this area.

Latin America & Caribbean

Brazil

Commentary on existing case law

In Brazil, the law on employee monitoring derives from constitutional principles, such as an individual's privacy and intimacy, (as discussed more fully in the 'Summary of existing legislation') and Superior Labour Court case law, the highest level of the labour courts in Brazil. Apart from case law on employee monitoring through cameras installed by employers in bathrooms and private areas, the decisions on monitoring the use of telephone, Internet, corporate emails and other communication systems by the employer are scarce in the Superior Labour Court.

Brazilian case law states that employers may monitor the use of communication systems provided by the employer to the employee (e.g. telephone, internet, corporate email system and other communication systems), if it is expressly stated in internal policies or employment agreements, that such systems are work tools, and consequently to be used for business purposes only. It is essential that the possibility of such monitoring is fully communicated to all employees so they are aware they have no privacy rights whilst using the communication systems provided by the employer whilst at work.

Case law is inconsistent regarding the use of the corporate email system to send personal emails while at work. In practice, most employers adopt the policy of monitoring the corporate email system subject to the employee's acknowledgement that he/she has no privacy rights or expectation of privacy regarding emails sent and received through employers' email accounts, addresses (corporate email system) and equipment (for instance, notebooks, etc.) provided by the employer.

It is important to highlight that, according to case law, this surveillance cannot be done on personal telephone calls and/or personal email accounts, but only in telephone calls related to work and in the corporate email system. Thus, it is strongly advisable that employers do not access employees' personal email accounts at work, since it would be considered a violation of privacy, subject to indemnification in court. To avoid security breaches of personal emails, it is very common to forbid the use of personal email accounts at work.

Security cameras are also allowed by Brazilian labour courts' case law in public areas of the work place, but the employee must be aware of their presence and the cameras cannot be set in places where they can violate an employee's intimacy (for instance, bathrooms, etc.).

Trends that can be identified

As mentioned previously, Brazilian case law concerning the monitoring of employees' corporate emails, asserts that access by the employer will not be considered a violation of employees' privacy and intimacy if the employer has an internal policy or an agreement held with the employee expressly stating that the computing resources are a tool for work. This policy should state that the employee does not have any privacy in it, and he/she is aware of the fact that there is no expectation of privacy in the use of the employer's computing resources granted for work-related use.

There are already decisions issued by Brazilian labour courts recognising that email is specifically a work tool even without an internal policy expressing this. As such those claims for damages resulting from the employer's access to employee's emails are found to be groundless.

Existing case law

List of cases

1. *Soraya Maria Drago Thorpe v. Correio Braziliense S/A*, Case number TRT-RO-00105-2004-016-03-00-0 (page 262)
2. *Vânia Moreira do Carmo v. Telemar Norte Leste S/A. and BH Telecom Ltda.*, Case number TRT-RO-00105-2004-016-03-00-0 (page 263)
3. *Elielson Lourenço do Nascimento v. HSBC Seguros Brasil S.A.*, Case number TST-RR-613/2000-013-10-00.7 (page 264)
4. *Gustavo Francisco Bastos v. MBM Recuperações de Ativos Financeiros S/C Ltda.*, Case number TST-AIRR-1.542/2005-055-02-40.4 (page 265)
5. *Jorge Luís Arroyo Durand v. Cia. Palmares de Hotéis e Turismo*, Case number TST-AIRR-1640/2003-051-01-40.0 (page 266)
6. *Adenise Brito de Souza v. KR Indústria e Comércio Ltda.*, Case number TST-AIRR-1142-35.2012.5.05.0008 (page 267)
7. *Clevis Soares da Silva v. Minerva S.A.*, Case number TST-AIRR-557-82.2016.5.23.0091 (page 268)

Case Name, Citation, and Court	Soraya Maria Drago Thorpe v. Correio Braziliense S/A, Case number TRT-RO-00105-2004-016-03-00-0 Regional Labour Court of the 10th Region (Federal District and the State of Tocantins)
Date	28 January 2004
Subject	Pain and suffering damage; employer monitoring; violation of privacy
Key facts	<ul style="list-style-type: none"> The former employee, who was hired as a telephone operator, claimed indemnity for pain and suffering alleging that her privacy, intimacy, and honor were violated because her private calls were monitored by the employer.
Key points	<ul style="list-style-type: none"> The Regional Labour Court accepted the employer's argument that the telephone terminals were work equipment of the former employee and the routines that should be followed for the performance of the employment agreement were monitored by the employer through a phone log which the former employee was aware of. Therefore, there was no violation of the privacy, intimacy, or honor of the former employee. In addition, there is no violation of the secrecy of telephone conversations as the communication equipment was a work tool. By making private telephone calls during work hours and being aware that the employer was monitoring the conversations by means of the speakerphone, the disclosure of her private issues was a risk that the former employee took. As the employer's fault or intent to offend the employee was not demonstrated, there was no pain and suffering in the circumstances.

Case Name, Citation, and Court	Vânia Moreira do Carmo v. Telemar Norte Leste S/A. and BH Telecom Ltda., Case number TRT-RO-00105-2004-016-03-00-0 Regional Labour Court of the 3rd Region (State of Minas Gerais)
Date	3 September 2004
Subject	Employer's abuse of its managing and inspecting power; pain and suffering damage; excessive inspection of work through phone log and recording of telephone conversations.
Key facts	<ul style="list-style-type: none"> The former employee claimed pain and suffering damage under the allegation that her privacy, intimacy, and honor were violated due to the excessive inspection of her work as the employer used a phone log and recorded her telephone conversations.
Key points	<ul style="list-style-type: none"> The Regional Labour Court accepted the former employee's allegations on the ground that the employer's conduct in creating an embarrassing and vexatious situation was unlawful. Notwithstanding the employer's managing and inspecting power, such an abusive exercise of the management and inspection is inadmissible as it involves compromising the privacy, the intimacy and even to the honor of the employee, resulting in injury to the dignity of the worker as a human being, which is an evident violation of constitutional principles.

Case Name, Citation and Court	<i>Elielson Lourenço do Nascimento v. HSBC Seguros Brasil S.A., Case number TST-RR-613/2000-013-10-00.7</i> Superior Labour Court
Date	18 May 2005
Subject	Corporate email; termination for cause; dissemination of pornographic material; lawful evidence.
Key facts	<ul style="list-style-type: none"> The employer terminated the former employee for cause after it was found that the former employee, during work, sent emails with pornographic photos using the employer's computer and provider, as well as using the employer's electronic address that had been made available to him to perform his professional tasks. The former employee alleged that the evidence that supported his termination for cause was unlawful because it was obtained through violation of his email, without his consent.
Key points	<ul style="list-style-type: none"> The Superior Labour Court ruled that only the personal or private emails of the employee, sent through his own email provider, are protected under the Constitution. On the other hand, a corporate email is a work tool supplied by the employer to the employee for work purposes. The misused corporate email (for instance, to send pornographic photos) may cause losses to the employer. As this case involved corporate email destined for work only, the employer had the right to access the Internet and the provider. In addition, an employer is liable before third parties for the acts of its employees during work and has the right to protect its image. When an employee is given an email box by the employer, for corporate use, and is previously warned that only professional messages are acceptable, the employee has no reasonable expectation of privacy. An employer may monitor and track the employee's activities in the workplace, that is, check his messages. Evidence produced through such means is not unlawful to support termination for cause in cases where the employee sends pornographic material to a co-worker. There was no violation of article 5, items X, XII, and LVI, of the Federal Constitution.

Case Name, Citation and Court	Gustavo Francisco Bastos v. MBM Recuperações de Ativos Financeiros S/C Ltda., Case number TST-AIRR-1.542/2005-055-02-40.4 Superior Labour Court
Date	4 June 2008
Subject	Unlawful evidence - employer accessing the corporate email box supplied to an employee. No denial of the right to be heard.
Key facts	<ul style="list-style-type: none"> The former employee alleged he had his right to be heard denied in the case, alleging that the emails produced by the employer in its defense were supposedly obtained upon access to the corporate email account of the former employee.
Key points	<ul style="list-style-type: none"> The Regional Labour Court considered that the evidence was lawful, because it was an access, by the employer, to the content of the corporate email supplied to the former employee for him to perform his professional duties. It was stated that the supply of an email box by the employer to its employees on its premises is to enhance the efficiency of their jobs toward the performance of the corporate purpose of the company. Therefore, it is a work tool to be used with the same diligence devoted to any other work tool. The employee must use it safely and properly, and respect the purposes for which it is intended. As a subscriber of the Internet access provider, the company is responsible for its use in compliance with the law. If the employee occasionally uses the corporate email account for private matters, he should do it aware that its access by the employer is not a violation of his personal mail, or violation of his privacy or intimacy, since it is equipment and technology supplied by the employer to be used in work and to meet the company purposes. Thus, the use of the evidence resulting from the access to the email box supplied by the employer was not a denial of the right to be heard.

Case Name, Citation and Court	<i>Jorge Luís Arroyo Durand v. Cia. Palmares de Hotéis e Turismo, Case number TST-AIRR-1640/2003-051-01-40.0</i> Superior Labour Court
Date	15 October 2008
Subject	Corporate email account; access by the employer without employee consent; unlawful evidence not characterized.
Key facts	<ul style="list-style-type: none"> The former employee alleged the nullity of the use of the content of his corporate email account to prove the termination for cause enforced on him.
Key points	<ul style="list-style-type: none"> According with the Superior Labour Court, with the understanding adopted in said Court, the corporate email account has the legal nature of a work tool, supplied by the employer to its employee. For such reason, the worker must use it properly, aiming at more efficiency in the services he renders. Thus, the use of the content of this work instrument by the employer does not violate Articles 5, Items X and XII of the Federal Constitution; an employer has to take care of the proper use of the facilities it supplies for its employees to perform their duties. Therefore, the right to intimacy of the former employee was not violated.

Case Name, Citation and Court	<i>Adenise Brito de Souza v. KR Indústria e Comércio Ltda., Case number TST-AIRR-1142-35.2012.5.05.0008,</i> Superior Labour Court
Date	27 May 2015
Subject	Termination for cause; violation of company data; email monitoring; no violation of intimacy and mail confidentiality.
Key facts	<ul style="list-style-type: none"> The former employee sued for the reversal of the termination for cause, alleging that the evidence supporting such dismissal was obtained illegally, once the employer monitored her emails. Therefore, it violated her intimacy and the mail confidentiality, which are rights guaranteed by the Federal Constitution.
Key points	<ul style="list-style-type: none"> The Regional Labour Court concluded that the employer, in the scope of its management power (Article 2 of the CLT), can take steps in order to ensure that the employees meet their commitment to work. However, it must do so by always respecting the fundamental rights of workers, among which is the right to intimacy. The alleged violation of the intimacy and of the mail confidentiality — guaranteed in Article 5, Items X and XII of the Federal Constitution — did not occur, because it was not a personal email account. As revealed by the evidence, the monitoring took place concerning the corporate email account, and the appellant/defendant was aware of that fact. In such situation, the courts have adopted the position that there is no violation of said constitutional principle, when, for instance, the employee uses the corporate email to receive and send material of a pornographic nature. The Superior Labour Court upheld the decision of the Regional Labour Court that the intimacy and mail confidentiality of the former employee were not violated.

Case Name, Citation and Court	Clevis Soares da Silva v. Minerva S.A., Case number TST-AIRR-557-82.2016.5.23.0091, Superior Labour Court
Date	6 December 2017
Subject	Pain and suffering damage; Surveillance cameras in an employees' locker room; Violation of personality rights.
Key facts	<ul style="list-style-type: none"> The former employee claimed pain and suffering damage under the allegation that there was a surveillance camera in the men's locker room, equipment that caused him embarrassment and violated his privacy.
Key points	<ul style="list-style-type: none"> The Superior Labour Court granted the case to the claimant under the argument that the damage, in such a situation (installation of cameras in the locker rooms) is presumed, in that the capture of images of the employee while in the locker room, a space for private use by nature, exposes the employee to embarrassment and intimidation and violates the dignity of the human being, even though the images were never disclosed.

Summary of existing legislation

In Brazil, there is no specific law regarding employees' privacy or data protection. Therefore, the subject is ruled by the general Federal Constitution principle under which the individual's privacy and intimacy are protected, as follows:

"Article 5 - All persons are equal before the law, without discrimination of any nature, and Brazilians and foreigners residing in the country are ensured with the inviolability of the right to life, freedom, equality, safety and property, as follows:

(...)

X - the privacy, private life, the person's honor and reputation are inviolable, whereas violation of said rights assures the right to the resulting pecuniary damages for pain and suffering.

(...)

XII - the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable, except, in the latter case, by court order, in the cases and in the manner prescribed by law for the purposes of criminal investigation or criminal procedural finding of facts; (...)"

The individual personality civil right (in which a private life is included in this concept) is also protected according to the Brazilian Civil Code:

"Article 20 - Except with authorization, or if necessary for the administration of justice or to maintain public order, the disclosure of written, the transmission of the word, or the publication, exhibition or use of a person's image may be prohibited upon his/hers request and without prejudice to compensation when appropriate, affecting his honor, good name or reputation, or intended for commercial purposes. (...)"

"Article 21 -The person's private life is inviolable and the judge, upon request by the interested party, shall adopt the required arrangements to prevent or cease any act opposing to this rule."

It is also of note that the Law no. 12,965/2014 (Brazilian Internet Act) establishes principles, guarantees, rights and duties regarding the use of the internet in Brazil, such as:

- the inviolability the of user's intimacy and private life, as well as the secrecy of their communication through the internet;
- the protection and non-disclosure to third parties of the user's personal data, except through their express consent; and
- the clear and complete information about the collection, use, storage and protection of the user's data, which cannot be done in violation of the applicable legislation and must be expressly agreed by the user.

The law does not explicitly mention that the provisions above are also applicable to employees, but as much as possible, if such information will be disclosed or stored by third parties, it is advisable to obtain the employee's free and informed consent.

Future legislation which may have an impact on employee monitoring

This is not applicable for Brazil, given the lack of relevant future legislation that may impact on the topics addressed in this document.

New and Emerging Technologies

New forms of collaborative communication channels

The emergence of new forms of communication channels already poses a challenge for employers looking to protect themselves by way of employee IT monitoring.

This can be seen in the difficulties employers have at present in carrying out disciplinary investigations where traditional workplace communications channels have not been used. An example we advised on recently was misconduct by a group of employees whose team leader had set up and encouraged the use of a WhatsApp group to exchange messages, including the ability for employees to swap shifts with one another. However, outside the scope of the employer's system and not properly checked by the team leader, serious misconduct and bullying took place within the Group over a period of months, until such time as a complaint was finally made to the employer.

In seeking to carry out the disciplinary investigation, the employer was then faced with attempts by the employees to argue that this conduct was within their private lives and nothing to do with the workplace. This complicated what was already a difficult situation involving misconduct by a number of employees.

With the proliferation of alternative communication channels which may be used informally by employees, including emerging services such as Slack, it is vital for employers to address the risks these new channels present.

Employers should adopt clear policies, applied rigorously in practice, that only permitted work equipment or devices (which can be the subject of monitoring) can be used for work purposes and for the exchange of work-related information and that the non-work communication channels may not be used for non-work-related purposes.

Such rules should be drafted broadly so as to cover new forms of communication channels which might emerge, rather than being specific to existing channels.

Bring your Own Device (BYOD)

BYOD is not a particularly new practice. However, the risks for an employer associated with BYOD use have increased in recent years with the proliferation of smart phones and the number of employers permitting their workforce to use their own devices in the course of their work.

The risks associated with BYOD have been well-documented including by the UK Fraud Advisory Panel's guidance on BYOD policies⁴⁰ and by the ICO in its Bring Your Own Device guidance.⁴¹ These both provide essential guidance to employers who permit BYOD arrangements. Clearly, different forms of BYOD exist and the data may be stored either on the device, on a server within the employer's IT network (or private cloud) or a combination of these.

The ICO guidance makes clear that the data controller must remain in control of the personal data for which he is responsible at all times, regardless of the ownership of the device used to carry out the processing. Guidance is also provided in the context of employee IT monitoring.

Key issues which require to be considered will typically include:

- what type of data is held;
- where data may be stored;
- how it is transferred;
- potential for data leakage;
- blurring of personal and business use;
- the device's security capacities;
- what to do if the person who owns the device leaves employment; and
- how to deal with the loss, theft, failure and support of a device.

Two key points that emerge from the guidance are:

- the use of BYOD must not introduce vulnerabilities into existing secure environments; and
- every employer should have an effective BYOD policy in place which sets clear rules and responsibilities in relation to the use of BYOD at work.

A policy by itself however is insufficient and an important component of any BYOD policy should be ongoing audit and monitoring of compliance.

Further recommendations include:

- regardless of where the data is stored, employers must take appropriate measures to protect against

⁴⁰ Fraud Facts, Issue 23, June 2014

⁴¹ https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

unauthorised or unlawful access, for example, secure access credentials, if the device is lost or stolen;

- such measures can include controlling access to the data or device using a password or PIN or encrypting the data; the device being automatically locked if inactive for a period of time; access being locked or data deleted if an incorrect password is entered a number of times;
- setting appropriate default security controls which must not be altered by employees (or requiring these to be set and verified before BYOD may be used) alongside clear rules such as never using the device to send company data using non-corporate systems (or potentially certain types of sensitive data at all);
- since BYOD generally involves the transfer of data between the personal device and the employer's corporate system, the transfer process itself presents risks such as a so called "*man in the middle attack*" or other types of interception – as such, forcing all traffic through an encrypted channel such as a VPN is advisable;
- some platforms also allow the monitoring of data transferred for data leakage and loss – which may be highly relevant in the context of the risk of insider-threat from employees;
- addressing the risk of data loss or unintended disclosure that can arise from human error, such as employees sending emails to the wrong email address, which again technological solutions now exist for. One example is the CheckRecipient software⁴² which uses artificial intelligence to check the emails employees send and ensure they are correctly addressed;
- providing guidance and training to employees on their responsibilities and what they can do to maximise security at all times, for example, in relation to the installation of apps from untrusted sources, or how to assess the security of WiFi networks;
- linking the use of BYOD through corporate networks to a clear Acceptable Use Policy and Social Media Policy; and
- being able to locate devices and remotely and securely delete data held on them such as through using Mobile Device Management (**MDM**) technology.

The ICO guidance also highlights the need for employers to consider how to manage employees who might "root" or "jailbreak" devices, which might remove some of the default security controls that have been put in place.

Alongside any technological ability to detect such actions, employers should set clear expectations that any employee not complying with the BYOD or associated policies, may face disciplinary action up to and including dismissal. All policies should be backed up by appropriate training and refreshers for all staff, so awareness is maintained.

BYOD of course presents particular issues in the specific context of employee IT monitoring. By definition, employees will be making personal use of their own device. Technical measures adopted by an employer to protect its personal data may increase the level of workplace monitoring that occurs. Examples include the monitoring of all internet traffic or the geo-location of personal devices, which can be tracked using MDM software, even if the device has not been reported stolen.

⁴² <https://www.checkrecipient.com/>

We have experience advising clients on these issues, using the geo-location of devices as part of, for example, measures to ensure the safety and security of those who carry out lone working or who provide services to those in the community.

Other employers will use such technology to enable them to quickly allocate resources to the right locations or may use vehicle telematics. The rise of the gig economy provides clear examples in the context of Uber drivers or Deliveroo couriers.

However, this could be extended, for example, to analyse how long employees are spending at their desks or other work locations, through the monitoring of BYOD devices.

As noted above, all employee monitoring needs to comply with the restrictions within existing UK data protection law, which requires fair processing for specified purposes and for monitoring to be transparent and proportionate.

Where possible, steps should be taken to maintain clear separation between the personal data processed on behalf of the data controller and that processed for the device owner's own purposes. Otherwise, monitoring technology must remain proportionate and not excessive, especially in relation to periods of personal use, for example, this might include evenings and weekends. It is also important to keep monitoring to the specified purpose and not, for example, used for ongoing surveillance or monitoring of users.

The further requirements discussed in relation to GDPR also need to be considered in terms of existing and future BYOD monitoring.

The use of a LIA should allow the business need to be weighed against the impact on personal privacy and considering any alternative options which exist to ensure the correct balance is struck in relation to BYOD monitoring.

We would not anticipate that this assessment should present a difficulty where pressing business interests apply (such as addressing insider-threat risk or risk to the security of systems and company data) provided proper account is taken of personal privacy issues and any safeguards are implemented that ensure the monitoring is proportionate.

Big data, artificial intelligence (AI) and machine learning

The development of better AI potentially provides employers with a powerful tool in order to learn more about their employees. We are likely to see the deployment of AI to better monitor employee communications and activities in order to detect or predict behaviours which may be non-compliant with an employer's policies and procedures.

For employers looking to minimise the risks posed from insider threat, this will clearly be of interest insofar as this might allow them to pick up earlier signs of aberrant or unusual behaviour or activity which might suggest some potential security risk to an organisation. This potential risk may or may not come to pass but may provide such an organisation with the ability to target a form of closer monitoring.

In the UK case law review, a recent example can be seen in the case of *Various Claimants v. Wm Morrisons Supermarket plc*. There the claimants argued that their supermarket employer ought to have realised at an earlier stage that the wrongdoer employee posed a security risk to the organisation, given his behaviour. Reliance was placed on the fact that the individual had searched for information regarding The Onion Router (**TOR**), so he would be able to browse the internet undetected, albeit he was prevented from being able to install it due to firewalls deployed in their systems. However, on the facts of that case, this search in itself did not raise a red flag regarding the individual nor any need for closer monitoring, which in turn the claimants relied upon.

AI which can learn and recognise patterns or indicators of behaviours that may suggest individuals present risk is likely to be of interest to employers, subject to employee monitoring law. For example, a bank or similar institution will wish to be aware of any concern that arises in relation to its traders or other individuals in similar roles, with the ability to damage the organisation.

An example of this using big data cited in a recent ICO's discussion paper,⁴³ is the use by HMRC of their Connect system used to identify potential tax fraud by bringing together over a billion items of data from 30 sources, including self-assessment tax returns, PAYE, benefits, tax credit data, DVLA, credit card sales and social media.

This however, requires to be legally compliant and in particular (under UK law) amount to fair, transparent and proportionate data processing. This relates both to any personal data being used for this purpose and any personal data generated by it.

In addition, the legal restrictions in relation to automated decision-making and profiling (such as those discussed in relation to GDPR) may also be relevant and require to be complied with. The examples often cited in this context are refusing credit by automated decision making and e-recruitment decisions being made without human intervention.

As outlined above, individuals have a right under GDPR not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. As increasing use is made by employers of user-entity behaviour analytics to spot changes in user behaviour which might point to insider threat, there is a need to understand and comply with the legal restrictions.

⁴³ Big data, artificial intelligence, machine learning and data protection (September 2017) pp 35-36 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>

The specific restriction on automated decision-making in itself is unlikely to be an issue where the automation in itself does not give rise to legal or similarly significant effects. This is likely to be the case where the analytics only flag unusual behaviour for further human consideration and review. As such, no decision (for example, as for the need for a disciplinary investigation) is being taken by the operation of the analytics, other than a decision that further human review is necessary.

That being the case, it is perhaps the separate requirements within GDPR as to fair, transparent and proportionate processing that need to be carefully considered and complied with in respect of user-entity behaviour analytics.

Users will have to be made aware of the nature of the monitoring which is taking place and understand how this impacts them. The need for proportionality requires also that the legitimate business aims stand up to scrutiny and are not overridden by the rights of individuals and that those aims cannot be delivered in a less invasive way. Questions of the sensitivity of such analytics might arise and the level of false positives that might be generated.

This raises the separate issue of the need for personal data to be accurate (a requirement under existing UK data protection law as well as GDPR). Within data analytics, even if the data is reported accurately; this does not necessarily mean the inferences or conclusions drawn from it are accurate in respect of the individual concerned. Automated flags that point towards an employee posing a risk of insider threat activity may well be inaccurate in relation to that individual and this may give rise to further issues where it leads to decisions being taken, such as implementing a higher level of more intrusive monitoring in respect of their use of IT systems, all of which proves unnecessary.

Note also the right of individuals to seek access to the personal data held on them, including that obtained from such analytics.

Moreover, as noted above, GDPR requires a Data Protection Impact Assessment (**DPIA**) to be carried out in certain instances likely to create a high risk to people's rights and freedoms particularly when the processing uses new technologies. It also places a requirement on data controllers to incorporate privacy by design and default into data processing.

Beyond the context of data protection, a risk of discrimination can also arise where the big data itself leads to flags which are tainted by discrimination (for example, outside the employment context, the example of a consumer being refused credit based on discriminatory profiling).

The ICO discussion paper notes that companies are going to have to be both more transparent and more accountable for what they do with personal data and that this is no different for big data, AI and machine learning. It suggests that data protection should not be seen as the barrier to data analytics and rather that privacy should be embedded within big data analytics and that doing so will foster benefits such as encouraging trust. The overall ICO message is that the benefits of big data and AI to companies will not be met at the expense of data privacy rights.⁴⁴

⁴⁴ Big data, artificial intelligence, machine learning and data protection (September 2017), Foreword

Biometric monitoring

We anticipate similar issues arising in relation to the scope for employers to use biometric information for monitoring purposes in future. This might arise, for example, from an employer using AI to analyse voice waves of its employees on telephone conversations (whether recorded or not), to detect any concerns which might arise (e.g. from voice tone).

This might also extend to the use of other biometric data, such as fingerprints or retina scanners which could be deployed by an employer for monitoring purposes, including for security related or performance reasons. An example might be an employer using such technology to monitor when employees scanned in and out of particular areas of a work location, for example, to see if designated break times were adhered to.

Clear issues are likely to arise here under the issues of proportionality and also from biometric data being "special category" data for GDPR purposes, which as we have seen, can only be processed in very limited circumstances.

We foresee tension continuing to arise in future between the benefits that new monitoring technology might offer and the privacy restrictions highlighted above, with GDPR imposing particular restrictions which need taken account of.

Social media analysis

We are likely to see wider collection of social media output by individuals, in order for companies to carry out better people analytics. Companies such as DataSift⁴⁵ currently offer Human Data Analysis to the market, using data from a wide variety of social media platforms including Twitter, Facebook and many others.

Within the employment context, some employers currently make use of publicly available social media posts, as part of their standard recruitment process, but without taking proper account of the legal restrictions that would prevent such activity.

The key risks in this respect arise (in the UK) from data protection law and potential claims under the Equality Act 2010.

The Equality Act 2010 is relevant as an unsuccessful candidate may argue they were not offered a role due to a protected characteristic (for example, a disability not relevant to the role, or a religious belief, or sexual orientation) found on their social media profiles or posts, which would not have been apparent to the employer had they not accessed that content.

Similarly, as we have seen, data protection law requires fairness, transparency and proportionality. So, for example, the ICO's Employment Practices Code (in relation to the current requirements of the Data Protection Act 1998) is clear that candidates for employment are required to be expressly told of any vetting that will be carried out and that vetting should only be used as a means of obtaining specific information (for example, a Criminal Record Bureau check for posts for which this is required), not as a means of general intelligence gathering.

The Code also provides that vetting should be carried out only where there are particular and significant risks involved to the employer, clients, customers or others and where there is no reasonably practicable alternative.

The issue of social media vetting was also recently addressed by the WP29 Opinion on data protection at work, which is worth setting out as it clearly shows how supervisory authorities such as the ICO are likely to view such data processing.⁴⁶

"Use of social media by individuals is widespread and it is relatively uncommon for user profiles to be publicly viewable depending on the settings chosen by the account holder. As a result, employers may believe that inspecting the social media profiles of prospective candidates can be justified during their recruitment processes. This may also be the case for other publicly available information about the employee.

However employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to process those data for their own purposes. A legal ground is required for this processing, such as legitimate interest. In this context, the employer should – prior to the inspection of a social media profile – take into account whether the social media profile of the applicant is related to business or private purposes, as this can be an important indication for the legal admissibility of the data inspection. In addition, employers are only allowed to collect and process personal data relating to job applicants to the extent that the collection of those data is necessary and relevant to the

⁴⁵ <https://datasift.com/>

⁴⁶ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, see pp. 11-12.

performance of the job which is being applied for ...

... The individual must also be correctly informed of any such processing before they engage with the recruitment process."

WP29 then gives a worked example of an employer who checks publicly available social media profiles as part of recruitment and states that only where candidates have been informed of social media vetting and where this is necessary for the job would an employer potentially be able to rely upon legitimate interests as a fair ground for processing this personal data.

It contrasts this with a further worked example, where an employer monitoring the LinkedIn profiles of former employees for the duration of their non-compete clauses, with the purpose of monitoring compliance with those clauses. So long as that employer can prove such monitoring was necessary to protect legitimate interests and that the former employees were adequately informed about the extent of regular observation of their LinkedIn profiles, WP29 considers the employer may be able to rely upon legitimate interests.

In summary, the restrictive limitations placed on social media vetting, are likely to make it difficult for employers to lawfully do so, unless there are both lawful grounds – in terms of legitimate interest applying – as well as transparency.

We expect to see challenges arising in this area from unsuccessful job applicants, where they consider a breach of their data protection rights have taken place. This might arise where a job opportunity is withdrawn as a direct consequence of an undisclosed social media check highlighting concern.

The same limitations, so far as data protection law is concerned, would of course apply to employers making use of social media output in relation to their existing employees. Employers may wish to consider addressing the transparency requirement by being clear within social media policies that such access may take place, if there are legitimate interests in doing so (for example, which might include alleged misconduct outside work which impacts the employer).

Dark web monitoring

The Dark Web is an increasing source of concern to companies, with reported growing popularity and mainstream press coverage highlighting its existence. It is also well documented that this has created growing concern for IT security practitioners. This is not least because the Dark Web provides an opportunity for insider-threat activity to be carried out. Reports last year highlighted, for example, the trend of cybercriminals to use the Dark Web to spend considerable resources to recruit insiders, with purposes including to steal company data or plant malware or compromising system security.

From an employee IT monitoring point of view, the same legal considerations discussed above apply to Dark Web monitoring. As such, monitoring requires to be fair, be on lawful grounds and be transparent and proportionate.

In terms of applying the legitimate interest test, we consider that an employer will clearly have a legitimate interest in seeking to prevent employees from bypassing the Surface Web and using browsers/configurations in an attempt for their activity to be anonymous. It remains however key that this be achieved through proportionate and transparent means.

It should therefore be made clear to all employees within Appropriate Use policies that accessing the Internet other than using the programs and configurations provided by the employer will amount to a breach of those policies and being transparent that monitoring (as further specified) may be proportionately carried out to ensure compliance with this requirement.

Wearables

The recent WP29 report notes that employers are increasingly tempted to provide wearables to their employees to track and monitor their health and activity within and sometimes outside the workplace. The report states that insofar as this will involve the processing of health information by the employer it would be prohibited under GDPR.

This arises from it being highly unlikely that employees are able to provide legally valid consent given the unequal power within the employment relationship. That being the case, it is difficult to see what other special category condition could be satisfied and in relation to which the employer could argue that such processing would be necessary.

The WP29 report gives the example of an employer which has gifted fitness monitoring devices to its employees, which devices can provide information including as to steps taken, heartbeat and sleeping patterns over time. It states:⁴⁷

"The resulting health information should only be accessible to the employee and not the employer. Any data transferred between the employee (as a data subject) and the device/service provider (as data controller is a matter for those parties).

As the health data could also be processed by the commercial party that has manufactured the devices or offers a service to employers, when choosing the device or service the employer should evaluate the privacy policy of the manufacturer or the service provider, to ensure that it does not result in the unlawful processing of health data on employees".

A strict approach is also taken to the question of the aggregated data only being provided by the service provider to the employer:

"Even if the employer uses a third party to collect the health data, which would only provide aggregated information about general health developments to the employer, the processing would still be unlawful ... it is technically difficult to ensure complete anonymisation of the data. Even in an environment with over a thousand employees, given the availability of other data about employees the employer would still be able to single out individual employees with particular health indications such as high blood pressure or obesity"

The clear view appears to be that if wearables are provided by an employer, the processing of health data should generally be confined to employees accessing that information. Where an employer is seeking aggregated data, the issues noted above and question of complete anonymisation would require to be carefully considered in each case.

The same issues in relation to fair, transparent and proportionate processing will also arise here. Employers will required to make their employees aware prior to issue, of how their personal data will be processed in connection with the use of wearables and, for example, the measures that are in place to safeguard the privacy of health information.

⁴⁷ Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p. 18

United Kingdom Annex – detailed case reports

United Kingdom Annex – detailed case reports

Case Name, Citation and Court	<p><i>Avocet Hardware v. Morrison EAT/417/02</i> Employment Appeal Tribunal</p>
Date	23 September 2004
Brief outline of facts	<p>M was employed by A as a telesales operative. Without M's knowledge, A monitored his calls. When A took exception to one of M's calls with a customer, M was dismissed summarily for gross misconduct.</p> <p>M brought an unfair dismissal claim to an employment tribunal. In defending this claim, A sought to adduce as evidence the contents of that particular phone call which it had recorded, as justifying its decision.</p> <p>The employment tribunal ruled that this evidence was inadmissible as it was obtained in breach of the Regulation of Investigatory Powers Act 2000 s.1 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.</p> <p>A appealed against this decision to the Employment Appeal Tribunal (EAT).</p>
Outcome and key aspects of reasoning	<p>The EAT accepted A's evidence might have been obtained in breach Article 8, this did not necessarily lead to the conclusion that it could not be admitted in proceedings.</p> <p>A's right to a fair trial under Article 6 had to be considered, because the contents of the telephone call were crucial to their justification for dismissal, it has to be admitted into the evidence regardless of the method by which it was obtained.</p>

Case Name, Citation and Court	<i>McGowan v. Scottish Water EAT/0007/04</i> Employment Appeal Tribunal
Date	23 September 2004
Brief outline of facts	<p>M was employed at S's water treatment plant and lived in tied accommodation nearby. S became suspicious that self-completed timesheets in respect to call out time submitted by M were being falsified by him.</p> <p>S considered how to best determine if these self-completed timesheets were in fact being falsified and considered the possibility of putting cameras inside the process plant, but this was deemed impractical. Therefore, S determined that covert surveillance should be carried out upon M for one week. Private investigators were employed who secreted themselves opposite the front door of M's house and filmed him coming and going.</p> <p>The results of that surveillance established that M had been submitting false timesheets and he was dismissed by S.</p> <p>M brought a claim of unfair dismissal, relying on the covert surveillance as rendering his dismissal unfair by reason of being in breach of his Article 8 right to private life.</p> <p>He was unsuccessful before the employment tribunal and appealed to the Employment Appeal Tribunal (EAT).</p>
Outcome and key aspects of reasoning	The EAT agreed that covert surveillance of a individual's home raised a presumption that the right to have one's private life respected was being interfered with. In this instance, however, the question of proportionality of the interference under Article 8(2) needed to be considered. The purpose of the surveillance was to witness how many times M left the house to go to the plant which would determine the accuracy of M's timesheets. Therefore, S's investigation went to the essence of the obligations and rights of a public corporation to protect its assets. S had considered other methods to investigate but did not deem any of these to be viable. As such the surveillance in this case was not disproportionate and EAT dismissed his appeal.

Case Name, Citation and Court	<i>Amwell View School Governors v. Dogherty EAT/0243/06/DA</i> Employment Appeal Tribunal
Date	16 June 2006
Brief outline of facts	<p>D was a teaching assistant and midday meals supervisor at A. D was subject to disciplinary proceedings and dismissed by A following hearings under that procedure, including D's appeal against her dismissal.</p> <p>The hearings were all attended by D and held before panels of governors, but attendance was limited to those directly connected to the investigations. Each hearing included, or was followed by, private deliberations by the panel members. Minutes of each hearing (aside from the private deliberations) were prepared by the school secretary.</p> <p>D brought a tribunal claim for unfair dismissal. Following a standard case management direction for disclosure of documents, D disclosed of a list of 145 items which included three items described as "records" of the three hearings.</p> <p>At the tribunal hearing it was discovered that these items were covert recordings D had made of the hearings without the knowledge of the panel members. A objected to the inclusion of these items as evidence on the grounds of inadequate prior disclosure and the "<i>clandestine</i>" nature of the recordings. The Tribunal ordered that the hearing should be adjourned and that D should pay the costs already incurred, but that these items could be included at the rescheduled hearing, provided that the actual recordings and transcriptions were disclosed to A in advance.</p> <p>A appealed the tribunal's case management order to the Employment Appeal Tribunal (EAT).</p>
Outcome and key aspects of reasoning	The EAT recognised that the tribunal was clearly convinced that the recordings were directly relevant to D's case. The EAT rejected A's submission that the tribunal had erred in law in admitting evidence which had been disclosed late, finding that the tribunal's exercise of discretion to control its own proceedings through the case management order as outlined above, was a reasonable response to the situation.

	<p>The EAT agreed with the tribunal that the recordings had been made clandestinely, but not illegally. A had failed to provide a specific authority to support why the recordings should be excluded on this ground.</p> <p>The EAT also rejected A's submission that the evidence should be excluded on broadly the same public policy grounds as would justify the exclusion of evidence of what occurred at hearings in private of any judicial or quasi judicial body and/or during the private deliberations of such a body as it would be contrary to the "<i>public interest</i>".</p> <p>It held that the governors were simply acting in the same capacity as a panel of senior managers of any other employer and exercised no obvious judicial function.</p> <p>However, it accepted that D could not use parts from the private deliberations in her evidence. It concluded that there was an important public interest that parties should comply with the "<i>ground rules</i>" on which disciplinary and appeal proceedings were based stating:</p> <p><i>"No ground rule could be more essential to ensuring a full and frank exchange of views ... than the understanding that their deliberations would be conducted in private and remain private".</i></p> <p>The EAT did however indicate this public policy could potentially be overridden in exceptional circumstances, for example, where the private deliberations disclosed evidence of discriminatory conduct.</p>
--	---

Case Name, Citation and Court	Copland v. United Kingdom (2007) 45 EHRR 37 European Court of Human Rights
Date	3 April 2007
Brief outline of facts	<p>C was employed as an administrator at a further education college in the UK.</p> <p>On the deputy principal's orders, C's telephone, internet and email use were monitored in order to ascertain whether she was using them excessively for personal use. This was done without C's knowledge. At the time, the college did not have a policy on monitoring employees' communications. C contended that her personal movements, both at work and when on leave were the subject of surveillance and that legally privileged materials were seen by the deputy principal who was subsequently suspended.</p> <p>There was a dispute between the parties as to the nature and extent of monitoring. C claimed that her calls were monitored for at least 18 months, and her emails for at least six months. This was denied with it being accepted only that monitoring took place only over a period of a few months. There was also dispute as to whether incoming calls were being monitored, and as to the extent of information being recorded.</p> <p>C challenged this surveillance as breaching her rights under Article 8 and brought proceedings to the European Court of Human Rights.</p>
Outcome and key aspects of reasoning	<p>The ECtHR confirmed that telephone calls from business premises were <i>prima facie</i> covered by the terms "<i>private life</i>" and "<i>correspondence</i>" for the purposes of Article 8(1). It logically followed that emails sent from work and information derived from the monitoring of personal internet usage should also be protected under Article 8(1).</p> <p>On the basis that C did not know that her work calls, emails or internet usage were being monitored, the court stated that it was reasonable for her to expect that her privacy would be respected.</p> <p>Even if the monitoring was not as extensive and intrusive as C claimed, the collection and storage of C's personal information which there was acceptance had taken place without her knowledge would itself amount to an interference with C's Article 8 rights. The Court had to, therefore, determine whether that interference was "<i>in accordance with the law</i>"</p>

	<p><i>and necessary in a democratic society</i>" and, as such, permitted by Article 8.</p> <p>As when these incidents took place, there was no domestic law at that time in the UK regulating monitoring of communications, and as the college had no policy informing employees that they could expect such monitoring to take place, the interference was not "<i>in accordance with the law</i>" and Article 8 had therefore been violated.</p> <p>The court awarded C EUR 3,000 for non-pecuniary damage and EUR 6,000 for costs and expenses</p>
--	---

Case Name, Citation and Court	<p>Fosh v. Cardiff University EAT/412/07</p> <p>Employment Appeal Tribunal</p>
Date	23 January 2008
Brief outline of facts	<p>F was a university professor working for the respondent university, C. F supported a student, S, in bringing a claim of race discrimination against C. F continued to represent S despite the fact that the university asked him to stop given in their view it amounted to a clear conflict of interest. In addition F was accused by C of disclosing confidential information to S.</p> <p>Disciplinary proceedings were commenced against F, during which time he was suspended. The disciplinary investigation involved a search by C of F's email account.</p> <p>F was dismissed and the findings included inappropriate communication with students via email and inappropriate involvement with the student who had made a race discrimination claim against C.</p> <p>F claimed unfair dismissal, victimisation under the Race Relations Act 1976 and automatically unfair dismissal for whistleblowing under the Public Interest Disclosure Act 1998. The tribunal found that F's dismissal on grounds of misconduct to be procedurally fair and to fall within the range of reasonable responses. It also found that there was no victimisation on racial grounds. Finally it concluded that there was no breach of the Public Interest Disclosure Act by C.</p> <p>F appealed to the Employment Appeal Tribunal (EAT) alleging also that the dismissal was unfair by virtue of the email monitoring being in breach of Article 8.</p>
Outcome and key aspects of reasoning	<p>The EAT dismissed the appeal. The tribunal had made a clear and unequivocal finding of fact that the reason the respondent took action against the claimant was a perceived conflict of interest and breach of confidentiality.</p> <p>In relation to the claim of victimisation, the EAT was satisfied by the university's non-discriminatory explanation for the treatment of F.</p> <p>Finally, the EAT decided that C would not have breached Article 8 ECHR if it was an "<i>emanation of the state</i>". F's emails were searched in accordance with the university's internal rules and further C could</p>

rely on the Regulation of Investigatory Powers Act 2000. The employment tribunal had properly taken these matters into account when deciding whether Article 8 applied.

Case Name, Citation and Court	Turner v. East Midlands Trains Ltd [2012] EWCA Civ 1470 CA Court of Appeal
Date	16 November 2012
Brief outline of facts	T was employed by East Midlands Trains Ltd as a senior train conductor. She was dismissed for fraudulently selling faulty tickets and dishonestly keeping the proceeds. She was unsuccessful in claiming unfair dismissal, ultimately appealing to the Court of Appeal, which in its judgment gave guidance on the application of Article 8 in the context of an unfair dismissal claim.
Outcome and key aspects of reasoning	At the Court of Appeal, T argued that the consequences of her dismissal engaged her Article 8 rights under the ECHR as it resulted in damage to her reputation caused by a finding of dishonesty; the potential restriction on her ability to obtain other employment as a result of that finding; and damage to the social relationships with work colleagues. T argued that the Tribunal should, have adopted a " <i>proportionality</i> " test under Article 8(2). rather than applying the traditional " <i>band of reasonable responses</i> " test for unfair dismissal. The Court noted that each of the alleged consequences set out above could in principle engage Article 8. The Court confirmed the case law principle that Article 8 may not apply where an individual brings the consequences complained of on themselves. However, it also noted that the case law confirms that an individual must have been shown to have committed any wrongdoing before that principle can be invoked. It also requires that the process leading to the determination of wrongdoing be conducted properly. The Court of Appeal stated that it cannot be proportionate to dismiss an employee with consequences that engage Article 8 in circumstances where the employer has reached that decision in a procedurally unfair manner. The Court however rejected T's main argument that there is a difference in the standards required under Article 8 and the " <i>band of reasonable responses</i> " test for unfair dismissal. Elias LJ, gave the leading judgment, found it " <i>very difficult to see how a procedure that could be considered objectively fair if adopted by a reasonable employer could nonetheless be properly described as an unfair procedure within the meaning of art.8</i> ".

Case Name, Citation and Court	<i>Smith v. Trafford Housing Trust [2013] IRLR 86</i> High Court
Date	16 November 2012
Brief outline of facts	<p>S worked as a Housing Manager for a private housing trust, T. He was a practicing Christian and occasional lay preacher. He posted a link on his personal Facebook page to a BBC news article entitled 'Gay church marriages set to go ahead'. His comments included, amongst others, that this was "<i>an equality too far</i>". There was an exchange of comments with colleagues from work who had access to the page as his 'friends' where he repeated his opposition. His Facebook page clearly identified him as working for T as a housing manager.</p> <p>T then received a complaint about these posts from one of these work colleagues, and brought subsequent disciplinary proceedings against S resulting in a finding of gross misconduct, for which T applied a reduction in pay and a demotion. They took the view that S's Facebook post gave rise to a breach of T's Code of Conduct and Equal Opportunities Policy and thereby amounting to gross misconduct on his part..</p> <p>T argued:</p> <ol style="list-style-type: none"> 1. S's conduct was such that it could bring T into disrepute; 2. S was promoting his own religious views, contrary to the Code of Conduct (and specifically dealings with customers and colleagues); and 3. Contrary to the Equal Opportunities Policy and Code of Conduct, S was failing to treat employees with dignity and respect, and was engaging in conduct that might make others feel uncomfortable, embarrassed or upset; <p>S issued proceedings in the High Court and brought a claim for breach of contract also alleging a breach of Articles 9 (freedom of religion) and 10 (freedom of expression) of the Human Rights Act 1998.</p>

<p>Outcome and key aspects of reasoning</p>	<p>The High Court found in favour of S. Taking each of the four arguments in turn:</p> <ol style="list-style-type: none"> 1. S's Facebook postings did not bring T into disrepute as it could not be concluded that the posts were made in any sense on T's behalf. It was clear that S used Facebook for purely social and personal reasons rather than for work purposes. It could not be said that a reader of T's views on gay marriage on his Facebook page would think any less of T for employing him as a manager. The views were held by T personally, posted on the weekend and done on his own Facebook page. 2. Given the right to freedom of expression and freedom of belief, individuals are entitled to manifest religious beliefs, as long as this is done lawfully. Although an employer would be entitled to prohibit promotion of religious beliefs whilst at work, it would be very unusual for an employer to attempt to impose such a prohibition on an employee in their personal life by means of a code of conduct incorporated into an employee's contract. S's Facebook wall was clearly not work-related; the Code of Conduct's prohibition on promoting religious views did therefore not extend to S's Facebook wall. 3. T had viewed the Code of Conduct and Equal Opportunities Policy requiring employees to treat colleagues with dignity and respect and to refrain from engaging in conduct which might make others feel uncomfortable, embarrassed or upset as covering all situations outside work where an employee came into contact with an employee. However the High Court held that adhering to this instruction would be a restriction on freedom of expression. Moreover, S's use of Facebook involved colleagues only because they had voluntarily chosen to be his Facebook friends and engage with his views online; this did not change the fact that his use of Facebook here was fundamentally personal and social. <p>In the circumstances, T did not have a right to demote S because of his Facebook postings and by doing so T was in breach of contract and S entitled to damages.</p>
--	---

Case Name, Citation and Court	<i>City and County of Swansea v. Gayle [2013] IRLR 768 (EAT)</i> Employment Appeal Tribunal
Date	16 April 2013
Brief outline of facts	<p>The respondent employer, S, was informed that their employee G had twice been seen playing squash at a sports club during work hours when he had not clocked out.</p> <p>As a response to this, S decided to investigate the allegation and hired a private investigator who secretly filmed G outside the sports club at times of the day when he was claiming to be at work. G was filmed a total of five times outside the sports club.</p> <p>G was subsequently dismissed but at an employment tribunal was successful in his claim for unfair dismissal. The tribunal found that although there were reasonable grounds for dismissal of G, the dismissal was unfair due to the surveillance that was carried out on him because 1) it was found that G's right to a private life under the ECHR was violated or 2) the local authority had ignored its obligations under the DPA 1998.</p> <p>The Tribunal found that the investigation was far more comprehensive than necessary and therefore unreasonable. The tribunal also felt that a person defrauding an employer still had an expectation of privacy in respect of those particular acts when carrying them out. S appealed to the Employment Appeal Tribunal (EAT).</p>
Outcome and key aspects of reasoning	<p>The EAT overturned the employment tribunal's decision. It said that surveillance on individuals in public places by taking photographs or video footage was not a breach of Article 8(1) because in such a situation there was no expectation of privacy. In this case, there was no breach of Article 8(1) because the video was taken in a public place and G was there when he should have been at work; the local authority was entitled to know where he was at that time.</p> <p>Furthermore, the EAT held that by committing fraud G could have no reasonable expectation that his actions were private. Whilst being photographed G was on his employer's time and as such he could not reasonably expect to keep private from his employer what he was doing.</p>

Case Name, Citation and Court	<i>Vaughan v. Lewisham LBC UKEAT/0534/12</i> Employment Appeal Tribunal
Date	6 June 2013
Brief outline of facts	<p>V. suffered from depression and complained of discrimination, harassment and victimisation whilst working for L. She based this on a number of communications over a lengthy period between herself and her colleagues. Her pleaded case referred to covert recordings V. said she had made. She gave accounts of each individual meeting and claimed that this could be verified by these recordings. Further, she said that these recordings could show that contemporary references made by L were inaccurate.</p> <p>These recordings were made by voice recordings and lasted approximately 40 hours. She brought her discrimination claims against L, the previous employer from where she had transferred and a number of colleagues.</p> <p>V. made an application to an employment tribunal to adduce the recordings in evidence but did not provide the tapes or transcripts of the discussions. The application was refused as V. could not satisfy the tribunal as to the relevance of any of the recordings. Admitting this evidence was seen as disproportionate given the length of the recordings and cost to the respondent of reviewing them.</p> <p>V. appealed to the EAT.</p>
Outcome and key aspects of reasoning	<p>The EAT upheld the decision of the tribunal, but for not the same reasons.</p> <p>The tribunal clearly had no means to form a view on the admissibility of any tapes, in the absence of the tapes or any transcripts. The EAT held however that while the Tribunal's order had been correct in those circumstances, it could not be said that any of the recordings would not to be admissible in evidence.</p> <p>It could easily have been the case that certain parts of the recordings were relevant and should therefore be admitted. Therefore, if V. were to make a new application to the employment tribunal, producing tapes and transcripts with a clear reason why they are relevant, then there may have been a different result.</p>

Case Name, Citation and Court	<i>Mason v. Huddersfield Giants Ltd [2013] EWHC 2869 (QB)</i> High Court
Date	15 July 2013
Brief outline of facts	<p>M was a rugby league player who was contracted to play for H for four years. His contract stated that he should maintain the rugby club's reputation and as such he should not conduct himself in a way that could bring the club into disrepute. At the end of the playing season he joined his team mates on a night out, during which a team mate took a picture of M's bottom using M's phone. The following day, M's girlfriend uploaded the picture to twitter, tagging another H player. As such over 4,000 twitter subscribers could view the picture. M deleted the tweet two days after it was uploaded.</p> <p>H terminated M's contract for gross misconduct, citing, amongst other things, that he was a role model for children who followed the club. Dismissing his appeal, the club also stated the need for players to use twitter and other social media platforms responsibly. Following this, M signed for another rugby league club for approximately half of his salary previously paid by H.</p> <p>M brought a claim to the High Court for breach of contract, challenging the conduct having been regarded as gross misconduct by H such that they were entitled to summarily dismiss him.</p> <p>M also claimed that his twitter account was purely personal and that there was no way that the tweet could be viewed as being on behalf of the club.</p> <p>It was also relevant that the club had recently recruited other players to M's playing position and there was evidence of them attempting unsuccessfully to sell him to another club prior to dismissal.</p>
Outcome and key aspects of reasoning	<p>The High Court held that M had not done anything deliberately and, at most, he had not promptly removed the photograph from his twitter posts. Moreover he had voluntarily taken the photo down only two days later without any request from the club.</p> <p>Although not conclusive, it was relevant that the conduct had taken place outside of work location and hours. H had stated that M's behaviour was not in keeping with the family values that H sought to</p>

encourage. However, the High Court had trouble reconciling this with the fact that the H had promoted an end of season drinking session, including the traditional 'naked run' for those players who had not scored a try during the season.

The High Court then considered the terms of the employment contract that M had with H; these focused more on the specifics of being a rugby player for H although the High Court recognised the fact that the values the club were seeking to uphold were important. However, misconduct by any player could only justify their dismissal if it either repudiated the contract or one of its essential conditions. M's conduct could not be seen as repudiation of his obligation to behave with decorum and dignity.

The High Court then attempted to put the tweets in context. They said that there was no obvious link from the twitter page to H and there was no biography on the twitter account describing M as a Huddersfield Giants rugby player.

As the twitter page was used predominately for personal and social rather than work related purposes there could be little reputational loss by the club if the page was enjoyed by reasonable readers.

It was also noted that there was never an apology issued by the club to its supporters who may have viewed the tweet, and such an apology would be an expected reaction if there was reputational damage as H claimed.

In the circumstances the club were not entitled to summarily dismiss him and he had been wrongfully dismissed.

Case Name, Citation and Court	Game Retail v. Laws EAT/188/14 Employment Appeal Tribunal
Date	3 November 2014
Brief outline of facts	<p>L was employed by G as a risk and loss prevention investigator, responsible for 100 of its stores in England. He opened a private Twitter account which did not identify him as a Game employee. However, he began to follow the Twitter accounts of the Game stores for which he had responsibility, in order to be able to monitor their tweets. 65 of those stores followed him back. G was notified in July 2013 by a store manager who was concerned about tweets posted by L on his private Twitter feed. An investigation took place and identified 28 tweets as being offensive in relation to dentists, caravan drivers, golfers, the A&E department, Newcastle United supporters, the police and disabled people.</p> <p>L was suspended and invited to a disciplinary hearing. G took the view he had posted offensive tweets on his Twitter account, thereby in the public domain and viewable by anyone on Twitter, including by Game stores that had chosen to follow him. He was dismissed for gross misconduct and his appeal was unsuccessful.</p> <p>He brought an unfair dismissal claim and he was initially successful. The Employment Tribunal found that the use of Twitter was not part of his role, all his tweets were unrelated to work and were made in his own time and apart from one work colleague, there was no evidence of anyone else being offended. G appealed this decision to the Employment Appeal Tribunal (EAT).</p>
Outcome and key aspects of reasoning	<p>The EAT allowed G's appeal. It was wrong to suggest that here L's Twitter followers were restricted to social acquaintances. Nor had the claimant made any use of the privacy restriction setting open to him in relation to his account. He could have, but chose not to operate two separate Twitter accounts, one for personal and one for professional purposes. 65 of G's stores had been following L and his offensive tweets would have been going out to them as well as any social acquaintances.</p> <p>The question of private usage was not irrelevant. A balance had to be struck between an employer's desire to remove or reduce reputational risk from social media communications by its employees and an</p>

employee's rights of freedom of expression. The EAT referred to *Smith v. Trafford Housing* and said that generally speaking, employees must have the right to express themselves, provided it does not infringe on their employment and/or is outside the work context. These questions might depend on the particular employment or work in question.

In this case, the Employment Tribunal had not properly taken into account that it did not involve private usage but tweets knowingly being sent without any restriction to an audience which included 65 of G's stores and the fact a member of staff felt sufficiently strongly to complain about the content. Although the Tribunal's decision could not safely stand, the matter was remitted by the EAT to a different Tribunal to be heard afresh.

Finally, the EAT declined to provide general guidance to be applied by Employment Tribunals in cases of this kind but recognised that a number of factors might be relevant such as whether the employer has an IT or social media policy, the nature and seriousness of alleged misuse, any previous warnings for similar misconduct in the past, actual or potential damage done to customer relationships and so on. However, laying down a list of criteria by way of guidance would run the risk of a tick-box mentality that is inappropriate in an unfair dismissal case.

Case Name, Citation and Court	<i>British Waterways Board (t/a Scottish Canals) v. Smith</i> UKEAT/4/15 Employment Appeal Tribunal
Date	3 August 2015
Brief outline of facts	<p>S was employed by B as a manual worker on a rota pattern under which he was on standby for one week in every five. Whilst on standby employees were not permitted to consume alcohol. S was unhappy in his job and brought a number of grievances against his colleagues in relation to bullying and harassment. While the grievances investigation was being carried out, the investigating officer found entries that S had made on his Facebook account from two years prior.</p> <p>These comments referred to drinking whilst on standby and also used highly offensive and disparaging language to describe colleagues. Following this, S was summarily dismissed following internal disciplinary proceedings. The stated reason for dismissal was that S's behaviour had undermined the relationship of trust and confidence, having made posts claiming he was under the influence of alcohol. This was in spite of the fact that the posts were made two years previously.</p> <p>S brought a claim for unfair dismissal. Although the Tribunal found that the disciplinary procedure had been fair, they also took the view that the failure to have regard to a number of mitigating factors, such as S's claim that a number of his comments posted online were not true, meant that the dismissal fell outside the band of reasonable responses for a reasonable employer. The dismissal was therefore unfair.</p> <p>B appealed, submitting that the tribunal had wrongly substituted its own views for that of the employer.</p>
Outcome and key aspects of reasoning	<p>The Employment Appeal Tribunal (EAT) upheld B's appeal, finding that there had been a reasonable investigation and a fair procedure and that B had a genuine belief that S was under the influence of alcohol whilst on standby. The fact that the actions of S had taken place some two years' prior was held to be irrelevant in the circumstances.</p> <p>The EAT found that the tribunal had substituted its own views for that of the employer, had made its own findings of fact about the potential risk arising from the actions of S and had also questioned the</p>

emphasis it had placed on the mitigating factors. Instead the Tribunal should have considered B's views about the events that had occurred and following this assessed whether the subsequent dismissal was within the range of reasonable responses. As there had been a reasonable investigation and fair procedure and the employer had lost confidence and trust in S, it was held that the dismissal was fair.

The EAT also commented on the circumstances of the case and the fact that it involved the use of Facebook. It confirmed that there was no special rules for such cases and they are to be determined in accordance with normal principles of law. In relation to this point, they referred to the judgment given by the EAT in *Game Retail Ltd v. Laws*.

Case Name, Citation and Court	<p>Garamukanwa v. Solent NHS Trust (EAT/245/15)</p> <p>Employment Appeal Tribunal</p>
Date	1 March 2016
Brief outline of facts	<p>G was a clinical manager for Solent NHS Trust (the Trust) and while working there formed a relationship with a female nurse, M. When the relationship broke down G began to suspect that M had commenced a relationship with another female colleague, S. He then embarked on a campaign of harassment and stalking. This involved him sending anonymous emails from a number of email addresses to work colleagues and members of management. M also became concerned that G was stalking her and complained to the police.</p> <p>The matter was investigated by the police who downloaded the emails from G's phone and disclosed them to the Trust. Following their investigation the police found that there were serious concerns over G's behaviour but no charges were brought.</p> <p>Having been provided with photographs found by the police which contained the emails sent, the Trust carried out a disciplinary hearing and G was dismissed for gross misconduct. In response, he claimed unfair dismissal but was unsuccessful.</p> <p>The Employment Tribunal found that the emails had an impact on work-related matters by having an effect on M's emotional stability and therefore performance at work – as such the decision to dismiss was within the range of reasonable responses and was fair. It held that Article 8 rights had not been engaged.</p> <p>G appealed to the Employment Appeal Tribunal (EAT), submitting that the emails he sent were private and the Trust had breached his Article 8 rights. He submitted that the Trust had failed to respect his family life by looking into matters relating fundamentally to his private life.</p>
Outcome and key aspects of reasoning	<p>The EAT had to first consider whether Article 8 had been engaged; it found that it had not been.</p> <p>Looking specifically at Article 8 the EAT said that the aspects of private life capable of being encompassed were very wide and could potentially include emails that were sent at work where the sender could expect a degree of privacy. However it was noted that this was</p>

	<p>very fact dependent in any given case.</p> <p>Although the tribunal was assessing a disciplinary investigation that related to a personal relationship between two colleagues, these were issues brought into the workplace by G's actions and also resulted in work-related issues. Furthermore, these emails were received by colleagues on work email addresses. The emails had had an effect on employees to whom G owed a duty of care, and also had an effect on the working relationship on the ward. The senior position that G held was also relevant as was the fact that he was subject to professional standards to behave in an appropriate manner. As such it was found that G had no reasonable expectation of privacy, and that he must have realised that the employee would complain of harassment.</p> <p>Even if Article 8 was engaged, any interference with G's Article 8 rights would have been justified by the Trust's need to protect the welfare of employees.</p>
--	--

Case Name, Citation and Court	<i>Barbulescu v. Romania [2017] IRLR 1032</i> European Court of Human Rights
Date	5 September 2017
Brief outline of facts	<p>B was employed as a sales engineer by a private company, S, in Romania. At his employer's request, for the purpose of responding to customer enquiries, he created an instant messaging account using Yahoo Messenger. The employer had internal regulations which strictly forbade the personal use of computers but which did not indicate any monitoring would take place. From 5 to 13 July 2007 S monitored B's communications in real time and alleged a breach of their internal regulations arising from B making personal use of Yahoo Messenger. Initially B denied he had made any personal use as alleged. S then provided B with a copy of a 45 page transcript of personal messages exchanged between B and his brother in law as well as messages exchanged with his fiancé over that period, some of which were of an intimate nature. On 1 August 2007, S terminated B's contract of employment.</p> <p>B challenged his dismissal in the domestic courts but was unsuccessful. He brought an application to the European Court of Human Rights (ECtHR) alleging that his dismissal breached his right to respect for private life and correspondence under Article 8 of the Convention.</p> <p>In a judgment of 12 January 2016, the Chamber of the ECtHR held that Article 8 was applicable but held there was no violation. The case differed from earlier cases such as <i>Copland</i> or <i>Halford</i> in that here the employer's internal regulations strictly prohibited any personal use taking place. The domestic courts had found the applicant to have committed a disciplinary offence. The employer had only accessed the content of communications after personal use had been denied by the applicant.</p> <p>B requested a referral of that decision to the Grand Chamber of the ECtHR which request was accepted.</p>
Outcome and key aspects of reasoning	The Grand Chamber agreed that Article 8 was applicable. Prior case law of the ECtHR recognised that the notion of " <i>private life</i> " was not restricted to an " <i>inner circle</i> " in which an individual may live his or her

	<p>personal life as they choose. It encompassed private life in a broader sense and included professional activities. Restrictions on an individual's professional life may fall within Article 8 when they have repercussions on the manner in which he or she constructs his or her social identity. It is in the course of working life that the majority of people have a significant if not the greatest opportunity to develop relations with the outside world. As regards the right to "<i>correspondence</i>", this had previously been held to extend to telephone conversations and emails sent from the workplace (see <i>Halford and Copland</i>). It was therefore clear from this case law that communications from business premises may be covered by both "<i>private life</i>" and "<i>correspondence</i>".</p> <p>Turning to the facts here, the applicant had been informed of the ban on personal use. However, it was not clear that he had been informed prior to the monitoring of his communications that this would take place. In any event, he was not informed in advance as to the extent and nature of the monitoring or that his employer would have access to the actual content of his communications.</p> <p>It was open to question whether and if so to what extent the employer's restrictive regulations left the applicant with a reasonable expectation of privacy. However, be that as it may, an employers instructions cannot reduce private social life in the workplace to zero. Respect for private life and correspondence continued to exist, even if restricted so far as necessary.</p> <p>The Court noted that its task in this case was to clarify the nature and scope of the positive obligation that a State party was required to comply with in order to protect the applicant's right to respect of private life and correspondence. Although Contracting States enjoyed a margin of appreciation in determining how to secure those rights, this discretion was not unlimited. Domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of those measures, is accompanied by adequate and sufficient safeguards against abuse. While the Court was aware of the rapid developments in this area, domestic authorities should treat the following factors as relevant:</p> <ol style="list-style-type: none"> 1. Whether the employee has been notified of the possibility that monitoring may take place. For measures to be deemed compatible with Article 8, the notification should normally be clear about the nature of monitoring and be given in advance. 2. The extent of the monitoring and degree of intrusion into the
--	---

	<p>employee's privacy. A distinction should be made between the monitoring of the flow of communications and their content. Whether all or part of communications have been monitored, whether the monitoring was limited in time and access restricted to a number of people, should all be taken into account.</p> <ul style="list-style-type: none"> 3. Whether the employer had provided legitimate reasons to justify monitoring communications and accessing actual content – since monitoring content is by nature more intrusive it requires weightier justification. 4. Whether it would have been possible to establish a monitoring system based on less intrusive measures than directly accessing the content of communications. 5. The consequence of monitoring for the employee subjected to it and the use made by the employer of the monitoring results. 6. Whether the employee has been provided with adequate safeguards, especially when the monitoring is of an intrusive nature – including that the employer cannot access the actual content of communications unless the employee has been notified in advance of that eventuality. <p>The question here was whether, in light of all the circumstances of the case, the Romanian national authorities struck a fair balance between the competing interests at stake, it being accepted that the employer had a legitimate interest in ensuring the smooth running of the company.</p> <p>As to how the domestic courts applied the above criteria, the Court had already concluded that B received no prior notification in advance of the extent and nature of his employer's proposed monitoring, or of the possibility that his employer might access the actual content of his messages. To qualify as prior notice, the warning from an employer must be given before monitoring activities are initiated, especially where they entail accessing the content of employee communications. International and European standards pointed in this direction requiring employees to be advised before any monitoring activities are carried out.</p> <p>Nor was the question of the scope of monitoring and degree of intrusion examined by the domestic courts, even though the employer recorded all B's communications in real time, accessed them and printed out their content. The domestic court has also not carried out a sufficient assessment of whether there were legitimate reasons to</p>
--	---

	<p>justify monitoring B's communications, including what specific aim could have justified such strict monitoring.</p> <p>Moreover, the domestic courts also did not consider the seriousness of the consequences of the monitoring for the employee – the applicant having received the most severe of disciplinary sanction – namely dismissal.</p> <p>Finally, the domestic courts failed to determine when the content of communications had taken place and whether this was only after the applicant denied personal use. In the view of the Court, accessing the content of communications at any stage of the disciplinary proceedings ran counter to the principle of transparency.</p> <p>In summary, the domestic courts failed to determine whether B had received advance notification of monitoring taking place and failed to have regard to B not having been advised of the nature and extent of that monitoring, or to the degree of intrusion involved. In addition, they failed to determine the employer's reasons for the monitoring and whether the employer could have used less intrusive measures in respect of that aim.</p> <p>Having regard to all these considerations, the Court found (by 11 votes to six) that there had been a violation of Article 8.</p> <p>No compensation was awarded on the basis that the finding of a violation represented just satisfaction.</p>
--	---

Case Name, Citation and Court	<i>Antovic and Mirkovic v. Montenegro [2017] ECHR 1068</i> European Court of Human Rights
Date	28 November 2017
Brief outline of facts	<p>A and M were professors within the School of Mathematics at the University of Montenegro. In February 2011, the applicants and other colleagues within the School were advised that video surveillance had been introduced in the seven amphitheaters in which classes were held. The stated aims were to ensure the safety of property and people, including students and the surveillance of teaching. Access to the data collected would be restricted by codes which would be known only by the Dean of the School.</p> <p>A and M complained to the Montenegro data protection authority seeking removal of the cameras claiming a breach of the applicable Montenegro legislation – the Personal Data Protection Act (PDPA). The regulator agreed and issued a decision requiring the cameras to be removed, which they were by 27 January 2012. In particular the regulator held that requirements of the PDPA had not been met as there was no evidence that there was danger to the safety of people and property in the auditorium and that the surveillance of teaching was not among the legitimate grounds for video surveillance permitted by the PDPA.</p> <p>In January 2012, the applicants commenced a compensation claim in the domestic courts for a violation of their right to respect for their private lives, by the unauthorised collection and processing of personal data relating to them. Both the Court of First Instance and, on appeal, the High Court found against the applicants. In doing so, they held that the university was a public institution, performing activities of public interest such as teaching and that it was not possible for video surveillance of the auditoriums, as public places, to violate the applicants' right to respect for privacy. It was a working area, like a courtroom or parliament where professors were never alone, therefore no violation of privacy could take place.</p> <p>The applicants submitted a complaint to the European Court of Human Rights that the unlawful installation and use of video surveillance equipment had violated their right to respect for private life under Article 8 of the Convention on Human Rights.</p>

Outcome and key aspects of reasoning	<p>The ECtHR held that Article 8 was applicable to the circumstances. It noted that it had previously held that "<i>private life</i>" may include professional activities and that it is in the course of their working lives that the majority of people have a significant, if not the greatest opportunity, to develop relationships with the outside world. Whether individuals have a reasonable expectation of privacy was a significant but not a conclusive factor.</p> <p>In the present case, the university amphitheatres were the workplaces of teachers. It was where the professors would not only teach students but also interact with them, thus developing mutual relations and constructing their social identity. The Court had previously held that covert surveillance of an employee at his or her workplace must be considered a considerable intrusion. It entails the recorded and reproducible documentation of a person's conduct at his or her workplace, which the employee was unable to evade. There was no reason why the Court should depart from that finding even in relation to non-covert surveillance. The Court had also previously held that even where an employer's regulations in respect of private social life in the workplace were restrictive, this could not be reduced to zero. Respect for private life continued to exist even if it might be restricted so far as necessary.</p> <p>Given their finding that the video surveillance in this case amounted to a considerable intrusion into the employee's private life, the question for the Court was whether this interference could be justified under Article 8(2) of the Convention. This requires the interference to be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society in order to achieve that aim.</p> <p>The Court held that as the video surveillance was not in accordance with domestic law – there having been no evidence put forward that surveillance was necessary for the safety of persons or property (as required by the PDPA) this requirement of Article 8(2) was not satisfied.</p> <p>This being the case there had been a breach of the right to respect private life under Article 8 and there was no need to further examine the other elements of Article 8(2) (including whether the aim was legitimate and the interference proportionate).</p> <p>The applicants were awarded EUR 1,000 each plus their costs (as assessed).</p>
---	---

Case Name, Citation and Court	Various Claimants v. WM Morrison Supermarket Plc [2017] EWHC 3113 (QB) High Court
Date	1 December 2017
Brief outline of facts	<p>Professional services company KPMG requested a copy of M's payroll data when carrying out an audit in 2012; S, an IT auditor, was employed to work on the project. In November 2013 following an internal disciplinary process, S downloaded the payroll data to a USB device. In December S then tried to use computer software capable of concealing the specific identity of a computer (known as The Onion Router or TOR) which had connected to the internet. In addition to TOR, S also created a false email account and used a pay-as-you-go telephone so that he could not be traced. Whilst on his home computer in January 2014, S posted a file enclosing the personal details of approximately 100,000 employees on a file sharing website. This data included employee names, addresses, national insurance numbers, bank sort codes, bank account numbers and salaries. Shortly after, links to the particular website were also posted elsewhere online.</p> <p>On 13 March, a CD containing a copy of the data was received by three newspapers in the UK. One of the newspapers, the Bradford Telegraph and Argus, notified M of the incident. M's management immediately took steps to remove the data, links to the website and ensure that the website had been taken down. S was later arrested on 19 March and charged with offences under the Computer Misuse Act 1990 and the DPA 1998.</p> <p>A number of employees whose personal details were affected by the data breach brought claims for compensation against M including under the DPA 1998. They also pointed to the claimant's behaviour at work in trying to conceal his actions as matters which should have alerted M to the potential for such wrongdoing to take place.</p> <p>The key issue for the High Court to determine was whether M was liable, directly or vicariously, for S's actions.</p>
Outcome and key aspects of reasoning	<p>The High Court found in favour of the claimants.</p> <p>In relation to primary liability under the DPA 1998, M was not the data controller in respect of the material posted on the internet and as such</p>

	<p>owed no duty to the claimants. However, M had failed to discharge its duty under the DPA 1998 to take measures to prevent unlawful disclosure and data loss. In the circumstances however, that failure in itself did not cause the disclosure, S having access to the data in the course of his duties. By the same reasoning M was not liable for breach of confidence or misuse of private information.</p> <p>On the facts the court accepted M's position that they could not reasonably have detected S's behaviour at work without carrying out monitoring which would be extremely time consuming and wholly disproportionate.</p> <p>However in relation to vicarious liability the High Court took a different approach. It was held that the internet postings were not disconnected from S's employment in time, place or nature. A determining factor was that M had specifically entrusted S with the payroll data and they had taken the risk in appointing him to the post where he would deal with this data. Furthermore, his role was to process data and disclose it to a third party; the ultimate non-authorised disclosure was in fact closely related to his role. Although the disclosures were made out of the office and outside of work hours this was not sufficient to break the chain connecting the disclosures to his employment. There was a sufficient connection between the role for which S was employed and his wrongful conduct.</p> <p>The High Court found that this conclusion was the same regardless of whether there was a breach of duty under the DPA 1998, a misuse of private information or a breach of confidence in that the acts constituting a legal wrong in each case were the same. The fact that M was actually the target of S's actions was also irrelevant and M should nevertheless be held vicariously liable for the actions of S.</p>
--	--

Case Name, Citation and Court	Lopez Ribalda and Others v. Spain Applications 1874/13 and 8567/13 European Court of Human Rights
Date	9 January 2018
Brief outline of facts	<p>The five applicants were cashiers working for a Spanish family-owned supermarket chain. In February 2009, their employer noticed stock level irregularities. In June 2009 steps were taken to install both visible and covert surveillance cameras. The visible cameras were aimed at customers and trained on the entrance and exit to the store. The covert cameras were aimed at employees and were zoomed in on checkout counters. Notice was given to employees of the visible cameras being installed but not the covert cameras. Later that month the five applicants were dismissed for their involvement in thefts or facilitating thefts.</p> <p>The applicants challenged their dismissals before the Spanish courts, arguing that their employer's use of covert video surveillance in the workplace without prior notice was unlawful. These challenges were not successful before the Spanish courts. The applicants then raised applications to the European Court of Human Rights alleging that the covert video surveillance violated their right to privacy protected by Article 8 of the Convention.</p> <p>They further complained that Article 6 of the Convention was breached insofar as the proceedings before the domestic courts had been unfair in that the covert video surveillance had been the main evidence relied upon to justify their dismissals.</p>
Outcome and key aspects of reasoning	<p>The ECtHR held that Article 8 was engaged by the facts. The covert surveillance of an employee at his or her workplace must be considered a considerable intrusion into his or her private life. It entails a recorded and reproducible documentation of a person's conduct at his or her workplace, which he or she, being obliged under the employment contract to perform the work in that place, cannot evade.</p> <p>Although the Spanish Government argued that the video surveillance was carried out by a private employer rather than the State, the purpose of Article 8 did not merely compel the State to abstain from interference in private life, there may be positive obligations inherent in an effective respect for private life. These obligations may involve the</p>

adoption of measures designed to secure respect for private life as between individuals. The question was whether the State had struck a fair balance between the applicants' rights to respect for their private lives and their employer's interests in protecting its property rights.

Turning to the facts here, the applicants' employer, in installing covert cameras, had not complied with the requirements within Spanish legislation on data protection. This required them to explicitly advise the applicants as to the personal data that would be processed on them. Not only that but the Spanish Data Protection Agency had issued an instruction clarifying that this required anyone using video surveillance to use a distinctive sign indicating the areas that were under surveillance.

In a situation where the right of every data subject to be informed of the existence, aim and manner of covert video surveillance was clearly regulated and protected by law, the applicants had a reasonable expectation of privacy.

Nor did the covert surveillance here target a prior substantiated suspicion against the applicants, so was not aimed at them specifically. The covert surveillance was aimed at all staff working on the cash registers over weeks, without any time limit and during all working hours.

The Court could not therefore accept the view of the Spanish courts on the proportionality of the measures taken by the employer. The rights of the employer could have been satisfied at least to a degree by other means such as informing the applicants of the installation of a system of video surveillance and providing them with the information required by Spanish data protection law. Having regard to these matters, the Court held that the domestic courts failed to strike a fair balance between the applicants' rights under Article 8 and their employer's interest in the protection of its property rights. Accordingly, there had been a violation of Article 8. The applicants were awarded EUR 4,000 each in respect of non-pecuniary damage.

However, the Court found no breach of Article 6: the question was whether the use of the evidence rendered the trial as a whole to be unfair. Here, all applicants had ample opportunity to challenge the authenticity and use of the material before the domestic courts, it was not the only evidence against them, and nothing was shown to support a conclusion that their defence rights were not complied with in respect of the evidence adduced.

67608

© 2018 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This document is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. We are providing information to you on the basis you agree to keep it confidential. If you give us confidential information but do not instruct or retain us, we may act for another client on any matter to which that confidential information may be relevant. Attorney Advertising. Please see dentons.com for Legal Notices.