Privacy and Data Protection: The Legal Framework

Kirsten Sjøvoll
4 March 2014

Introduction

Obtaining and disclosing information gives rise to a number of potential legal issues. In addition to possible criminal penalties, there are a number of civil causes of action which may be available to those who feel their private or personal information has been unlawfully obtained, stored, or used. Public authorities are of course bound to act compatibly with the Human Rights Act 1998 ("HRA"). The relevant articles when considering privacy, reputation and disclosure are Articles 8 (right to family and private life) and Article 10 (freedom of expression).

Public authorities may find themselves subject to judicial review if they act incompatibly with these provisions. In addition, section 8 HRA provides for a private law remedy in the form of damages. There are, however, a number of additional private law causes of action also available.

The principle causes of action which this paper will consider are:

- Claims under s.13 of the Data Protection Act 1998;
- Misuse of private information / breach of confidence;
- Claimants under the Protection from Harassment Act 1997.

Article 8 ECHR is incorporated into all of the above and will be relevant regardless of whether a public body is sued under the HRA itself. Additionally, paying public officials for information, or public authorities acting outside the scope of their powers may give rise to a tortious claim for misfeasance in public office, subject to being able to establish a deliberate intent to act unlawfully.

The Data Protection Act 1998

The DPA is the UK's "privacy statute". Section 55 makes it a criminal offence to unlawfully obtain or disclose "personal data", defined by s. 1(1) as data relating to an identifiable, living individual.

When processing personal data, public authorities **must** comply with the eight data protection principles which are as follows:

. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
. Personal data shall be accurate and, where necessary, kept up to date.
. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
. Personal data shall be processed in accordance with the rights of data subjects under this Act.
. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedules 2 and 3 of the DPA set out the purposes for which data may be lawfully processed:

. The individual who the personal data is about has consented to the processing.
. The processing is necessary: - in relation to a contract which the individual has entered into; or - because the individual has asked for something to be done so they can enter into a contract.
. The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
. The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
. The processing is in accordance with the "legitimate interests" condition.

These purposes are fairly wide and are non-cumulative. However, the guiding principle will often be one of fairness. In the case of *sensitive* personal data (e.g. medical information), public authorities must ensure that processing is for one or more of the purposes set out in Schedule 3:

. The individual who the sensitive personal data is about has given explicit consent to the processing.
. The processing is necessary so that you can comply with employment law.
. The processing is necessary to protect the vital interests of: - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or - another person (in a case where the individual's consent has been unreasonably withheld).
. The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
. The individual has deliberately made the information public.

- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

It may also be possible to process sensitive personal data where there is a substantial public interest in doing so.

Section 13 allows for individual compensation. It provides:

(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if—

(a) the individual also suffers damage by reason of the contravention, or

(b) the contravention relates to the processing of personal data for the special purposes.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.

To fall within the remit of s.13, the information in question must meet the definition of “data” in s.1(1) of the DPA, namely be processed by an automated electronic machine (by a computer or a tape recorder for

example), recorded with the intention that it will be processed in such a way, or alternatively recorded or be intended to be recorded as part of a "relevant filing system".

To come within s.13(1), a claimant must show that there has been a breach of the DPA by a "data controller". This is defined by the DPA as *"a person who […] determines the purposes for which and the manner in which any personal data are, or are to be, processed.*"

It is possible for information to be held manually but this must be as part of a "relevant filing system" if it is to be considered as "data" and caught by the Act. "Relevant filing system" is very narrowly defined and would, following *Smith v Lloyd Bank Plc* [2005] EWHC 246 (Ch), exclude information in "unstructured bundles kept in boxes" even if previously processed electronically. Unless, however, the information was held in an accessible and structured filing system such as a filing cabinet holding clearly and accessibly categorized files, it is extremely unlikely that the information would constitute data.

Section 13(1) requires a claimant to prove damage as a result of any breach. Following *Johnson v Medical Defence Union* [2007] EWCA Civ 262, damage in this context is limited to financial damage: injury to reputation or suffering distress will not suffice. Most Claimants will struggle to show that they have suffered financial damage: their claim will often relate to distress suffered as a result of personal information being accessed or made public.

Section 13(2) offers a means of bypassing the requirement for financial damage, as it allows claimants to sue for breaches of any of the Data Protection Principles where distress is caused, provided that it is related to the processing of that information for one of the special purposes. These are defined in s. 3 DPA as one or more of the following:

(a) the purposes of journalism,
(b) artistic purposes, and

(c) literary purposes.

These are unlikely to apply to public authorities. However, following the decision in *Vidal Hall and Ors v Google Inc* [2014] EWHC 13 (QB) it would appear that the courts are relaxing the rules on "damage" for the purposes of the DPA outside the context of the special purpose exemptions. The decision was on jurisdiction, rather than a full hearing on the merits but Mr Justice Tugendhat held that there was a "sufficiently arguable case" that the Claimants would be as entitled to recover damages for distress and anxiety under the DPA as they would for their claims for misuse of private information and harassment. The "moral" damage asserted could amount to sufficiently serious damage to engage their rights under Article 8 ECHR and was therefore at least in principle recoverable under the DPA.

It remains to be seen how the law will progress following *Vidal Hall* but on first view at least, it would seem that a significant hurdle to compensation claims under the DPA has been removed.

Breach of confidence

Breach of confidence can be relied on when one person misuses information which belongs to another.

The basic ingredients of this claim are well established. It is said to have three elements:

> *"First, the information itself must 'have the necessary quality of confidence about it'. Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it".*[1]

The information must have the "necessary quality of confidence" – it must not

[1] per Megarry J in *Coco v A N Clark (Engineers) Ltd* [1969] RPC 41 at 47.

be publicly available and it must not be "trivial or useless".[2] In practice, it will be difficult to protect non-personal confidential information" if it does not have some kind of commercial value. In order to constitute a claim for breach of confidence in relation to non-personal information it is usually necessary to demonstrate some actual or potential damage. This does not now seem to be limited to financial loss but may include distress.

The law will impose a duty of confidence in any situation where there is a "reasonable expectation of confidentiality."[3] Most cases are clear although there are, of course, some where there will be a reasonable difference of opinion.

The third element is the requirement for "misuse". It is now established that a claim for breach of confidence can succeed if all that happens is that confidential information is listened to or recorded but not further used or disclosed.

The case of *Imerman v Tchenguiz*[4] involved the accessing and copying of thousands of confidential documents held on computer. The purpose of these actions was to assist first defendant's sister, the wife of the claimant, in divorce proceedings. The defendants argued that there had been no "misuse". This argument was rejected by the Court of Appeal which held that a breach of confidence occurs where a defendant, without the permission of the claimant, "examines, makes, retains or supplies to a third party" copies of documents whose contents are (ought to have been) appreciated by the defendant to be confidential".[5] It is not a requirement that the defendant further misuses that information.

---

2 See *McNicol v Sportsman's Books* (1930) McG CC 116; *Attorney General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109.

3 *Imerman v Tchenguiz* [2011] Fam 116 [66]

4 [2011] Fam 116.

5 Ibid, [69].

Misuse of Private Information/Article 8 ECHR

Although English law does not recognise a tort of invasion of privacy[6] it does provide protection against the misuse of private information. The action for breach of confidence "absorbed" the rights protected by Articles 8 and 10 of the European Convention on Human Rights[7] and a new "tort" of "misuse of private information" was recognised.

The elements of the tort are well known and were summarised by the Court of Appeal in *McKennitt v Ash* [2008] QB 73, 81 [11] as follows:

> *"the court has to decide two things. First, is the information private in the sense that it is in principle protected by article 8? If "no" that is the end of the case. If "yes", the second question arises: in all the circumstances, must the interest of the owner of the private information yield to the right of freedom of expression conferred on the publisher by article 10?"*

Article 8 covers the right to "respect for family life, home and correspondence" and its scope has been the subject of much domestic and European case law.

The scope of "private information" is extremely wide. Aside from the obvious, such as health, or other intimate matters, business affairs[8] and even personal experiences that have been shared with others (which one party wishes to disclose) can come under the definition.[9]

Unlike the tort of breach of confidence, "trivial" information may also fall within the remit of Article 8 and give rise to an action for misuse of private information. This may include the taking of photographs in a semi-private place such as a hospital or a restaurant: *Murray v Big Pictures* [2009] Ch 481.

---

6 *Wainwright v Home Office* [2004] 2 AC 406

7 *Campbell v MGN Ltd* [2004] 2 AC 457 [17], per Lord Nicholls.

8 *Lord Browne of Madingley v Associated Newspapers* [2008] QB 103.

9 *McKennitt v Ash* at [28-30].

In *Copland v United Kingdom*, [2007] 45 EHRR 3, 7, the European Court held that the monitoring by an employer of an employee's telephone, email and Internet usage while at work – even though this did not include the *content* of those communications – without her knowledge was a violation of her right to respect for correspondence. Non-disclosure of that information in disciplinary proceedings subsequently brought against the employee was irrelevant.

In *Alison Halford v United Kingdom* [1997] 25 EHRR 523, the European Court of Human Rights held that telephone taps carried out on Ms Halford's office and home telephones by her employer, to gather material to assist in their defence against sex discrimination proceedings brought by her, were an unlawful violation of her Article 8 rights.

Of course, just because Article 8 is engaged does not mean that an interference is incapable of being lawful. However, the key question will always be whether the interference is *proportionate*.

Information sharing

In addition to gathering information, public authorities may wish to share the information obtained with others, including the media. They may wish to do so for perfectly legitimate reasons, for example to aid in the identification of an individual suspected of wrongdoing. However, aside from data protection concerns, this sort of information sharing also gives rise to issues in relation to misuse of private information and Article 8. Here, however, a further balancing exercise occurs in the form of the right to freedom of expression pursuant to Article 10 ECHR.

Again, the lawfulness of information sharing will be inevitably fact-specific. At one end of the spectrum is *Peck v United Kingdom* [2003] E.M.L.R. 15. The applicant in this case was suffering from severe depression as a result of personal and family circumstances. He walked down a busy main street with a kitchen knife and, upon stopping at a junction, attempted suicide by cutting his wrists. The entire incident was caught by CCTV cameras operated by the

local council. The man survived the suicide attempt but the images were subsequently released to the media by the council and published by two local newspapers. The footage was then provided by the Council to the BBC as well as to a local television news broadcaster. Although the Council had requested that the BBC did not display the applicant's face in the broadcast, they did so in the trailers for the programme and he was consequently identified by a number of his friends and family.

He brought judicial review proceedings against the council, alleging a breach of Article 8 and concurrently complained to the Press Complaints Commission. The European Court held that his Article 8 rights had been unlawfully interfered with by the council when they disclosed the CCTV footage to the press. The Court found that there was nothing to justify the disclosure and that no adequate safeguards had been put in place – such as seeking the applicant's consent, and ensuring that his identity would be masked not merely requesting it. Importantly, the Court found that in the context of disclosures aimed at crime prevention, particular care and scrutiny had to be applied.

This remains good law, and in the context of private individuals like Mr Peck, disclosure of information such as this is very likely to breach Article 8 and/or amount to a breach of confidence or misuse of private information. However, there is a grey area exacerbated by an increasingly less stringent approach to privacy taken by the European Court in recent years.

In *Von Hannover v Germany (No. 2)* app. No 40660/08, 60641/08, the Court found that the failure on the part of the German State, to grant an injunction preventing photographs taken of Princess Caroline while on holiday at a ski resort was not an infringement of her rights under Article 8. Guidance was given, however, and the following factors are relevant when deciding whether to disclose images to the media:

. **Whether the information contributes to a debate of general interest**

What amounts to “general interest” will depend on the circumstances of the case. However, the Court gave some guidance based on its case law as to what it generally considers is or is not a subject of general interest (rumoured marital difficulties of a politician or financial troubles of a famous singer being amongst those not found to be matters of general interest). [109]

. **How well known the person concerned is and the subject matter of the report**

The Court noted that private individuals may have a particular protection under Article 8 because there is a “fundamental distinction” between “reporting facts capable of contributing to debate in a democratic society, relating to politicians in the exercise of their official functions for example, and reporting details of the private life of an individual who does not exercise such functions.” [110]

. **The prior conduct of the individual concerned.**

In relation to this criteria, the fact that an individual has previously cooperated with the press may not serve as a trump card removing all protection against publication of the photo in question. [111]

. **Consent, form, and consequences of the publication.**

This may also include the scope of dissemination, the size of the publication, readership etc. [112]

. **The circumstances in which the photos were taken.**

Factors such as the consent of the subject, their knowledge that the photo was being taken, whether it was taken illicitly or through subterfuge will be relevant here. In addition, regard should be had to the “nature or seriousness of the intrusion and the consequences of publication” for the individual. An unknown, private individual may suffer a greater interference through publication of their image than a well known person, for example. [113]

The relevance of these factors to the types of information likely to be disclosed by local authorities will vary. Furthermore, the above factors were

recently followed by the European Court again in *Von Hannover (No. 3)* to again find no violation of Article 8 and further indicating a "lighter touch" in relation to privacy rights.

Nonetheless, members of the public not used to being in the public eye, may very well be viewed differently. For example, if a public authority conducts intensive surveillance upon a member of the public for a prolonged period of time, in semi private places, such as hospitals or restaurants, in circumstances where the evidence that they are guilty of any wrongdoing is slim, and takes numerous photographs as part of that campaign of surveillance it is suggested that it is more likely than not that (a) Article 8 is engaged; and (b) the interference with Article 8 will be disproportionate and so unlawful.

There may be additional harassment considerations which we set out below.

Harassment

Section 1 of the Protection from Harassment Act ("the Harassment Act") provides:

> ***Prohibition of harassment.***
> *(1) A person must not pursue a course of conduct—*
> *(a) which amounts to harassment of another, and*
> *(b) which he knows or ought to know amounts to harassment of the other.*
> *(2)For the purposes of this section, the person whose course of conduct is in question ought to know that it amounts to harassment of another if a reasonable person in possession of the same information would think the course of conduct amounted to harassment of the other.*
> *(3) Subsection (1) does not apply to a course of conduct if the person who pursued it shows—*
> *(a) that it was pursued for the purpose of preventing or detecting crime,*
> *(b) that it was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under any enactment, or*
> *(c) that in the particular circumstances the pursuit of the course of conduct was reasonable.*

An individual who feels they have been subject to harassment may apply for an anti-harassment injunction against a public authority or bring a civil claim for damages after the fact. Following *Vidal Hall* mere distress could suffice rather than any financial loss. However, the conduct complained of must be sufficiently unreasonable and oppressive before the court will find that it amounted to harassment. As to the appropriate test see: *Majrowski v. Guys and St Thomas's NHS Trust* [2007] 1 AC 224, per Lord Nicholls at [30] who said that to "… cross the boundary from the regrettable to the unacceptable the gravity of the misconduct must be of an order which would sustain criminal liability under section 2", and Baroness Hale who said at [66]: " … conduct might be harassment even if no alarm or distress were in fact caused. A great deal is left to the wisdom of the courts to draw sensible lines between the ordinary banter and badinage of life and genuinely offensive and unacceptable behaviour".

In *Ferguson v. British Gas Trading Ltd*, [2010] 1 WLR 785, the Court of Appeal held that although harassment was both a crime and a tort that did not modify in any way the constituents of the civil wrong and that since the individual was expected to tolerate a certain amount of annoyance, the impugned course of conduct had to be grave, in that it was oppressive and unacceptable, before either the criminal or civil law would intervene: per Jacob LJ at [17].

A public authority alleged to have committed the statutory tort or criminal offence of harassment may be able to rely on the defence provided for in s.1(3) of the Protection From Harassment Act. They would have to show that their course of conduct was (i) pursued for the purpose of preventing or detecting crime; or (ii) than in the particular circumstances the pursuit of the course of conduct was reasonsable.

However, following the recent Supreme Court decision in *Hayes v Willoughby* [2013] UKSC 17, the local authority must demonstrate that it held a "rational belief" that the subject of the conduct which would otherwise amount to

harassment had committed or was about to commit a crime. Rationality, according to Lord Sumption, differed from "reasonable" in the sense that the harasser must have:

"thought rationally about the material suggesting the possibility of criminality and formed the view that the conduct said to constitute harassment was appropriate for the purpose of preventing or detecting it." [15]

Without this, the required causal connection between purpose and conduct would be lacking. Per Lord Mance at [22]

"Mere unreasonableness is not the limit. But the law recognizes looser control mechanisms such as complete irrationality, perversity, abusiveness or, indeed, in some contexts, gross negligence"

These findings are consistent with the regime laid down by the Regulation of Investigatory Powers Act 2000 ("RIPA") which specifically governs information gathering techniques by public authorities. In relation to local authorities, in order for surveillance to be authorized the local authority must turn its mind to the seriousness of the offence, and keep it under review. It necessarily follows that there must be some rational basis upon which to embark upon a course of conduct which might, in some circumstances, amount to harassment.

Particular considerations in relation to public authorities and their employees

In contrast to the position in Strasbourg, the domestic courts have been generally more reluctant to find unlawful interference with an employee's private information through surveillance. Here, RIPA has been very much used as the starting point, rather than Article 8.

As discussed above, the 2012 Act means that directed surveillance of employees could only be conducted if it was in order to prevent the commission of a crime punishable by at least 6 months imprisonment. This

could conceivably cover the prevention and detection of fraud, for example where an employee is dishonestly claiming sick pay.

However, not all surveillance will be covered by RIPA. For example, in *C v The Police and the Secretary of State for the Home Department* (14th November 2006, No: IPT/03/32/H), the Investigatory Powers Tribunal ("IPT") held that video footage obtained by a private investigator employed by the police force to observe one of its employees who had brought a personal injury claim against his employer was not covered by RIPA. This was important because the Claimant's case hinged on the argument that the surveillance was unlawful because it occurred without authorisation. The IPT held that:

"The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers."

The key question for local authorities conducting surveillance on its employees seems to be whether that surveillance forms part of its core regulatory function. If it does not, it would seem that RIPA does not apply. This could be viewed as unsatisfactory as it appears to give local authorities a loophole through which to conduct more intrusive surveillance against its own employees than as against members of the public. Furthermore, if the surveillance occurs in a public place, it would appear that following the recent decision of the Employment Appeal Tribunal in *City and County of Swansea v Gayle* (16 April 2013) UKEAT/0501/12/RN, Article 8 may not be engaged at all.

Here, the Claimant was suspected of playing squash during work hours, for which he continued to receive payment. His employer conducted covert video

surveillance of the Claimant playing squash during work hours and accordingly dismissed him. The Claimant brought a claim for unfair dismissal arguing amongst other things that the process was unlawful because it was an unjustified interference with his right to private life under Article 8.

His claim was upheld at first instance but overturned on appeal to the EAT, which found that Article 8 was not engaged because surveillance had occurred in a public place, had occurred at a time when the Claimant was supposed to be working, and was conducted in order to establish that the Claimant was guilty of defrauding his employers, he had no reasonable expectation of privacy in respect of his activities. [23] The EAT went even further to say that, even if Article 8 was engaged, it was likely to be justified as necessary and proportionate in pursuit of a legitimate aim, which could either be described as the prevention of crime or the protection of the rights and freedoms of others. [23] In conclusion, where filming took place in public and there was no breach of RIPA, it would be extremely unlikely that Article 8 would be breached. [31]

In *McGowan v Scottish Water* [2005] ILR 167, the Claimant was suspected by his employer of falsifying his timesheets with regard to call out time. The Defendant thus decided to organize covert surveillance of Mr McGowan's home. This surveillance ultimately formed an important part of the evidence from which the Defendant took the decision to dismiss him. Mr McGowan contested the dismissal on the basis that the surveillance breached his Article 8 rights. This was rejected by the Employment Tribunal. The EAT upheld the first instance decision but on narrower grounds, finding that while *"covert surveillance of a person's home, unbeknown to him or her, which tracks all people coming and going from it…raises at least a strong presumption that the right to have one's private life respected is being invaded"*, in this instance, the interference was justified. The respondents were a public corporation, investigating what effectively amounted to fraud. Their behaviour was therefore not disproportionate.

The approach of the domestic courts, particularly the employment tribunals, does not sit well with the line of ECHR authority in relation to members of the public. This reflects the different philosophical considerations in relation to the reasonable expectations of privacy held by employees, who have contracted to certain obligations and which they may expect to have enforced against them if breached.

Conclusion

A range of civil remedies may be available for individuals who feel that their privacy has been breached by public authorities. The DPA is likely to apply in a range of situations common to public authorities, such as the retention of DNA by the police, the processing of personal information in adoption applications, or the provision of personal information across agencies. Article 8 is the guiding principle across all the available torts, and public authorities are held to a high standard when it comes to the private information of individuals.