11

The Right to Privacy

LOUISE MALLINDER

Introduction

Privacy is widely recognised in international and regional human rights law as a fundamental right that is necessary for the maintenance of liberal, democratic societies. This importance acknowledges that in addition to protecting an individual's personal life from public scrutiny, privacy protection can facilitate individuals' enjoyment of their political rights such as the right to religion, the right to freedom of association and the right to freedom of assembly. In recent decades, protection of the right to privacy within the UK has evolved to be a significant issue as the state has become a 'world leader' in using technologies such as biometric databases and surveillance cameras, and private actors, notably the media, have also used technological advances to gather information on individuals without their consent.

Despite the importance of the right to privacy and the growing pressures on individuals' enjoyment of this right, there is at present no comprehensive privacy law within Northern Ireland or the rest of the UK. Historically, the law of Northern Ireland offered only piecemeal protection for privacy, which a person could only rely upon indirectly. For example, suing someone for breach of confidence was possible provided that some private information had been misused or for defamation if material was published that was damaging to an individual's reputation. It was also possible to succeed in a claim of trespass or nuisance, particularly if private property had been invaded or the intrusion had been insistent and repeated. Similarly, individuals could seek some legal remedies where public authorities exceeded statutory regulations granting them the powers to breach individual privacy in specific circumstances defined as being in the national interest. However, these areas of tort law, equity law and public law protect distinct and specific interests rather than providing a general right to privacy.

With the full entry into force of the Human Rights Act 1998 in October 2000, the right to privacy contained in Article 8 of the European Convention on Human Rights (ECHR) became a direct part of Northern Ireland's law. Thus, for the first time, people in Northern Ireland could directly enforce their right to privacy against public authorities within domestic courts, rather than having to seek remedies at the European Court of Human Rights (ECtHR). However, the Human Rights Act 1998 is not directly enforceable against private bodies, such as the press. Instead, as with the pre-Human Rights Act era, individuals can still invoke their right to privacy against private actors only by relying on an existing cause of action, such as breach of confidence, which the courts can then interpret in light of Article 8 on the basis that the courts themselves are public authorities. As a result, privacy law in Northern Ireland remains a patchwork of the following legal provisions:

- general statutory provisions, such as the Human Rights Act 1998 and the Data Protection Act 1998;
- statutory regulations governing specific circumstances in which the state can lawfully intrude on an individual's privacy;
- common law rules, such as the laws on breach of confidence, defamation and trespass; and
- systems of informal regulation, such as the Press Complaints Commission.

Given the diversity of distinct legal provisions relating to the right to privacy in Northern Ireland, this chapter will not seek to survey each of them individually. Rather it will begin by exploring definitions of the right to privacy on the basis of Article 8. In the following sections, it will explore the extent to which people in Northern Ireland have access to remedies for violations of the right to privacy by public authorities and private actors. The latter section will focus primarily on the media because the actions of print media have produced voluminous case law on the right to privacy in recent years. For a complete picture this chapter should be read alongside Chapter 9 on freedom of expression and Chapter 10 on rights to access information.

What is the right to privacy?

The basis for the most general protection of the right to privacy in Northern Ireland's law is supplied by Article 8 of the ECHR, which reads:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being 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.

From this provision, we can see that although the term privacy is not defined, the Convention nonetheless seeks to protect an individual's privacy within broad, multiple and overlapping spheres of life. Each of these areas will be explored below. The right to privacy enshrined in Article 8 is not an absolute right. Instead, the Strasbourg case law has indicated that public authorities are permitted to limit the right to privacy provided that the interference is in accordance with the aims set out in Article 8(2). As a result of the incorporation of Article 8 into Northern Ireland's law through the Human Rights Act 1998, where a public body interferes with an individual's right to privacy outside these limits, it is acting unlawfully and can be sued by the victim.

Respect for private life

The ECtHR has described the right to a private life as 'a broad term not susceptible to exhaustive definition' (*Peck v UK*, 2003, para 57). However, from the case law it can be determined that the Court views the right as 'encompassing, inter alia, aspects of an individual's physical and social identity including the right to personal autonomy, personal development and to establish and develop relationships with other human beings and the outside world'. (*Evans v UK*, 2006, para 71)

The key areas within this right are protections for personal information, personal autonomy and physical integrity.

Personal information

The protection of personal information is often regarded as the core of ensuring respect for private life. It has produced a substantial body of case law from Strasbourg relating to the ways in which public authorities gather, store and use personal data (eg *Murray v UK*, 1994). This case law has focused on ensuring that states collect 'particularly sensitive or intimate data', such as that relating to sexuality (*Lustig-Prean and Beckett v UK*, 2000) or health (*Z v Finland*), or engage in covert surveillance (*Kopp v Switzerland*, 1998), only when there are compelling grounds to do so. The ECtHR has further found that respect for private life entails not just a negative obligation on the state to refrain from interfering in an individual's personal life, but also a positive obligation to take actions 'to secure effective respect for private life even in the sphere of the relations of individuals between themselves' (*Von Hannover v Germany*, 2004, para 57). However, states are afforded a 'wide margin of appreciation' in this area (*Mosley v UK*, 2011, para 108).

Within Northern Ireland, the Data Protection Act 1998 is the primary source of legal protection in relation to data processing, whether by public authorities or private actors. The Act sets out the circumstances in which data can be processed and establishes eight principles for data protection. These require personal data to be:

- processed fairly and lawfully;
- obtained for specified and lawful purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept any longer than necessary;
- processed in accordance with the rights of the individual(s) involved;
- kept securely; and
- not transferred to any other country unless adequate protection is in place there.

The Data Protection Act also creates a regulatory framework under which the Information Commissioner monitors compliance with the Act by individuals and organisations engaged in data collection. Failure to comply with this framework is a criminal offence. See Chapter 10 for more information on the Act.

In Northern Ireland the personal information of individuals who are in receipt of health or social care should be handled in accordance with the Code of Practice on Protecting the Confidentiality of Service User Information, which was issued in 2012 by the Privacy

Advisory Committee of the Department of Health, Social Services and Public Safety. Institutions wishing to make use of such personal information in Northern Ireland cannot benefit from the protection afforded by section 251 of the National Health Service Act 2006, which allows research to be authorised in certain circumstances even where an individual's consent has not been given. No equivalent legislation applies in Northern Ireland.

Personal autonomy

The right to a private life has also been interpreted by the ECtHR as embracing personal autonomy and personal development (eg *Pretty v UK*, 2002, para 61, where the Court said that a person's right to choose when to die engaged Article 8). This means that information concerning one's gender, sexual orientation and sexual life is considered to be private. For example, in *Dudgeon v UK* (1981), a case which went to Strasbourg from Northern Ireland, the Court found that legislation criminalising homosexual intercourse in Northern Ireland violated Article 8 as it prevented an individual exercising autonomy in his personal sexual preferences, and the state's justification for such a prohibition was disproportionate to the impact it had on the individual. In addition, personal autonomy can relate not just to the extent to which others intrude on an individual's choices but also to the extent to which an individual can retain control over his or her own body. The ECtHR has explored this issue in relation to questions of abortion (*Evans v UK*, 2006; *A, B and C v Ireland*, 2010) and assisted suicide (*Pretty v UK*, 2002). In the former cases, the Court found that states were entitled to a wide 'margin of appreciation' on the question of abortion as 'there is no consensus within the Member States of the Council of Europe, either as to the relative importance of the interest at stake or as to the best means of protecting it' (para 232). In relation to assisted suicide it found that Article 8 could be engaged with regards to 'quality of life' and the court was 'not prepared to exclude that this constitutes an interference with her right to respect for private life' (paras 52–54). However, the Court then ruled that: 'It is primarily for States to assess the risk and the likely incidence of abuse if the general prohibition on assisted suicides were relaxed or if exceptions were to be created.' It therefore held that the UK's criminalisation of assisted suicide was not disproportionate (para 74).

Bodily integrity

Finally, the right to a private life has been interpreted to include bodily integrity. While this incorporates an individual's right to freedom of choice regarding control over his or her own body, it also includes a right to freedom from physical intrusion, such as corporal punishment (eg *Costello-Roberts v UK*, 1995). In Northern Ireland's law, the state is empowered in certain circumstances to intrude upon bodily integrity. For example, under section 55 of the Police and Criminal Evidence (NI) Order 1989, the police are allowed to take intimate samples and to conduct strip searches, where they have reasonable suspicion that an individual may be carrying Class A drugs or objects that may cause harm to anyone. However, such searches must be conducted in accordance with requirements of Article 8.

Respect for family life

The ECtHR has interpreted the right to family life as offering protection to many different types of families. For example, in *X, Y and Z v UK* (1997), the Court found that the UK had not violated Article 8 when it refused to recognise a female to male transsexual as the father of a child who was conceived through artificial insemination from a donor. The Court did nonetheless conclude that due to the father's role in the child's life a family relationship between them did exist.

As with other elements of the right to privacy, the European Court has found that the right to a family life creates not only negative obligations on states to refrain from interference but also positive obligations to allow people to lead a family life. For example, in *Nurzynski v Poland* (2011), the Court found that where a person is being held in detention, the authorities are required to enable him or her to maintain contact with his close family. Furthermore, in *Abou v Romania* (2011), the Court held that the state violated Article 8 by forcing the applicant to leave Romania, where the public authorities had not acted in accordance with domestic law.

Respect for the home

The right to respect for the home clearly encompasses an individual's dwelling, but the ECtHR has also expanded this concept to include a person's office used for professional purposes (*Heino v Finland*, 2011). Where this right applies, it relates to an individual's right to occupy their home and their right not to be expelled from it. In addition, individuals have the right to privacy within their homes (see, eg *Bisir v Moldova*, 2011). However, in Northern Ireland's law, hundreds of pieces of legislation permit public authorities to enter private homes. These aim to protect the public welfare and prevent crime and include such laws as the Firearms Act 1968, the Misuse of Drugs Act 1971, the Criminal Law Act 1977, the Mental Health Act 1983, the Public Health (Control of Diseases) Act 1984, the Police and Criminal Evidence (NI) Order 1989 and the Fire and Rescue Services Act 2004. Within these laws there are inconsistencies relating to whether officials need to show warrants, whether they are permitted to use force, and what kind of penalties can be imposed on those who refuse them entry.

Respect for correspondence

Respect for correspondence applies, of course, to postal correspondence but today can also apply to other forms of communications such as emails, faxes or social networking. To date, case law from the ECtHR has focused on the right of a detainee to correspond with the outside world. For example, in *Milosevic v Serbia* (2011), the applicant complained that the prison authorities were opening and stamping all his legal correspondence, which the Court found not to be in accordance with the law. Within Northern Ireland, as will be discussed below, the Regulation of Investigatory Powers Act 2000 governs when and how some public authorities can intercept personal communications as part of their investigatory or intelligence functions.

Privacy, surveillance and public authorities

Although the right to privacy was incorporated into Northern Ireland's law by the Human Rights Act 1998, it has recently come under increasing pressure from the state. Technological advances have meant that it is now cheaper and easier for public authorities to collect, process and share considerable amounts of personal data, and the state can now use a wider range of surveillance tools, such as full-body scanners and CCTV cameras. One of the practical risks posed by such enormous data collection strategies in which large numbers of public officials may have access to information is that the data will not be kept secure. In recent years, several incidents have occurred in which copies of official databases containing the personal data of thousands of individuals have been lost or left in public places. In addition, state surveillance strategies often provoke political concerns as they could, for example, impinge on peaceful public protests. In such contexts, intrusions on the right to privacy could have negative repercussions on individuals' ability to exercise their political rights.

Under section 6(1) of the Human Rights Act 1998, 'it is unlawful for a public authority to act in a way which is incompatible with a convention right'. Furthermore, where persons believe that a public authority has violated their rights, section 7(1) permits them to 'bring proceedings against the authority ... in the appropriate court or tribunal' and to rely directly on their convention rights in those proceedings. When addressing complaints about interference with Article 8 rights courts are required to determine: (1) whether the interference was conducted in accordance with domestic law; (2) whether it was necessary to address public security or well-being; and (3) whether the measures taken were proportionate to the intrusion on the individual's right to privacy. In this way, it is possible for the courts to find that an individual's right to privacy was violated, but that such an intrusion was necessary and proportionate in the given circumstances.

This approach requires the courts to determine whether the public authorities appropriately balanced the rights of the individual against the public interest. How to strike this balance will depend in part on the severity of the public interest needs invoked. The state may find it easier to justify interferences based on national security (see *Leander v Sweden*, 1987, paras 58–67), than on crime prevention (see *Funke v France*, 1993, paras 53–57). Where a state interferes with privacy rights, it must ensure that there are safeguards to protect individuals from arbitrary interference, that the interference is conducted in accordance with the law, and that strict limits are placed on the power conferred (*Camenzind v Switzerland*,

1997, para 45). Assessments of the appropriateness of safeguards will measure the level of intrusion on an individual's privacy in relation to the importance of the national interests that the intrusion seeks to protect. This chapter will now explore how the balance has been struck in recent years in relation to: (1) stop and search powers; (2) the use of personal and biometric databases; (3) the use of closed-circuit television (CCTV); and (4) the interception of communications and surveillance.

Stop and search powers

Within the law of Northern Ireland, police officers are empowered to stop and search any person or vehicle under article 3 of the Police and Criminal Evidence (NI) Order 1989 provided that the officer has 'reasonable grounds for suspecting that he [or she] will find stolen or prohibited articles'. In addition, under the Terrorism Act 2000, section 89 empowers police officers to stop a person for as long as is necessary to question him or her about his or her identity and movements and what he or she knows about a recent explosion, a recent event endangering life, or a person killed or injured in a recent explosion or incident. If a person refuses to stop or answer questions, it is a criminal offence. Similar powers are provided in section 21 of the Justice and Security (NI) Act 2007, which grants both police officers and members of the armed forces the power to stop and question individuals about their identity and movements. According to statistics produced by the Police Service of Northern Ireland, the stop and search powers under these three pieces of legislation were used against 45,394 persons in a two-year period between 2009 and 2011.

The intrusion of privacy resulting from a similar power (conferred by section 44 of the Terrorism Act 2000) has triggered complaints to the ECtHR. In *Gillan and Quinton v UK* (2010) the applicants complained after being stopped and searched near to an arms fair in London in 2003. They initially challenged the police action through an application for judicial review, but they lost in the House of Lords (*R (Gillan) v Commissioner of Police for the Metropolis*, 2006). When the case reached Strasbourg, the ECtHR found that, although the stop and search powers were governed by domestic law

> the use of the coercive powers conferred by the legislation to require an individual to submit to a detailed search of his person, his clothing and his personal belongings amounts to a clear interference with the right to respect for private life. Although the search is undertaken in a public place, this does not mean that Article 8 is inapplicable. Indeed, in the Court's view, the public nature of the search may, in certain cases, compound the seriousness of the interference because of an element of humiliation and embarrassment (para 63).

The Court further considered whether the existing legal framework created sufficient safeguards to protect citizens. It found that 'there is a clear risk of arbitrariness in the grant of such a broad discretion to the police officer', and noted that such broad discretion, particularly where there is no requirement for 'reasonable suspicion', could result in the discriminatory use of the powers against minority populations or their misuse against peaceful protestors (para 85). Following this decision, the Terrorism Act 2000 (Remedial Order) 2011 was introduced in order to provide greater safeguards in the use of stop and search powers within anti-terrorism legislation throughout the UK. It is due to be replaced by a provision in the Protection of Freedoms Act 2012.

Personal and biometric databases

Public authorities within Northern Ireland and the UK, as in other developed countries, have increasingly constructed databases containing personal and biometric information. These databases are designed to facilitate law enforcement, combat terrorism, and enhance public sector service delivery. In addition, where public functions are outsourced to private actors, public authorities may share this personal data with private companies. The ECtHR considered the powers of state to collect personal data in *Leander v Sweden* (1987), where the applicant complained that his personal details had been stored on a secret police register for national security purposes, that this information had been shared with the navy so that the navy could vet employees, and that he had no opportunity to challenge the information. The Court found that

> in a system applicable to citizens generally, ... the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on

> which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life (para 51).

In this case, the Court held that the relevant domestic law contained detailed information on the procedures to be followed by the police when sharing personal data. When considering whether the measure was necessary, the Court noted 'the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it' (para 60), but it accorded the state a wide 'margin of appreciation'.

The issue of data sharing by public authorities was considered by the High Court of Northern Ireland in *Re O's Judicial Review* (2008). This case was brought by a police officer who alleged that a decision by the Police Ombudsman to require the Chief Constable to provide all medical and occupational health records relating to his medical condition violated his right to privacy. The applicant had been involved in shooting dead a member of the public and the Police Ombudsman was investigating the event. In reviewing the decision, the High Court found that, 'given the highly personal and sensitive data' requested by the Police Ombudsman, 'disclosure of that material without his consent would entail an interference with his right to respect for private life' (para 21). The court found that this intrusion was pursued for the legitimate aim of crime prevention (para 31), but it had not been carried out in a proportionate manner and hence violated Article 8 (para 54).

The legal authority for the police to take fingerprints and other bodily samples was conferred in England and Wales by Part 5 of the Police and Criminal Evidence Act 1984 (the PACE Act) and in Northern Ireland by Part 6 of the Police and Criminal Evidence (NI) Order 1989 (the PACE Order). The world's first National DNA Database was established in England in 1995. It was originally designed to contain the DNA records of convicted criminals, but its scope has since been considerably widened. By the Criminal Justice and Police Act 2001, which applied directly in Northern Ireland as well as in England and Wales, the database began to collect samples and data relating to persons who had not been prosecuted or who had been prosecuted but acquitted. It was further expanded by the Criminal Justice (NI) Order 2004 (mirroring the Criminal Justice Act 2003 for England and Wales), which allowed for 'non-intimate samples', such as rooted hair or mouth swabs, to be taken without consent. The 2003 Order also allowed DNA to be collected from persons who had been arrested, even if they were not later charged, and permitted any such sample to be retained indefinitely. Part 6 of the Police and Criminal Evidence (Amendment) (NI) Order

2007 made further changes to the police's powers. Northern Ireland now has its own DNA database, records from which are exported to the National DNA Database in England as well as being stored in Northern Ireland. By 2009, the Police Service of Northern Ireland held the profiles of 103,441 persons on its DNA database.

The compatibility of the National DNA Database with the ECHR was challenged unsuccessfully before the House of Lords in *R (S) v Chief Constable of South Yorkshire Police* (2004), but the case was then taken before the ECtHR as *S and Marper v UK* (2008) and the applicants won. One of the two applicants had been aged 11 when he was arrested for an offence for which he was later acquitted and the other had also been arrested but then acquitted. Both had had their DNA samples and fingerprints had been taken, and the police refused to delete these samples following their acquittals. In reviewing the case, the Court found that

> the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences ... fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. (para 125)

This decision was later endorsed by the UK Supreme Court in *R (GC and C) v Commissioner of Police for the Metropolis* (2011), which found that the excessive retention of DNA profiles violated Article 8. In addition, in *Re BBC (Attorney General's Reference No 3 of 1999)* Lord Phillips found that Article 8 would be violated by publishing that an individual's retained DNA 'has been used to link him to the commission of a crime of which he has been acquitted' (para 22). The UK government responded to the ECtHR's judgment by enacting the Crime and Security Act 2010. This established a range of time limits for the retention of biometric data depending on the seriousness of the offence, whether it resulted in a conviction, and whether the data was collected from a minor. In addition, the Minister of Justice in Northern Ireland has launched a public consultation on the deletion after three years from the Northern Ireland DNA Database of records relating to people who have been charged but not convicted.

Closed-circuit television (CCTV)

As frequently discussed in the media, the UK currently has a greater number of surveillance cameras than any other country. In 2011, research conducted by the Cheshire Constabulary estimated that there were 1.85 million CCTV cameras in the UK, a figure that equates to one camera for every 32 people. These cameras are operated by the police, local government and private organisations. Within Northern Ireland, according to the privacy campaign group *Big Brother Watch*, Belfast City Council alone operated 400 cameras in 2009. CCTV cameras have been widely installed for crime prevention and detection, the regulation of anti-social behaviour, and surveillance. In addition, speed cameras can match images with information in databases containing driver details and facial recognition features in order to ensure that drivers who are speeding can be fined. As a result of the prevalence of CCTV, individuals are often subject to surveillance without their knowledge.

Despite the widespread use of CCTV and its potential to intrude on individuals' right to privacy, its use is not currently regulated by a single legal framework. Where CCTV cameras are used to collect, process and store data (as opposed to simply displaying unrecorded live footage), they are governed by the Data Protection Act 1998, which applies to data collected by both public authorities and private actors. In addition, where public authorities use CCTV cameras for covert use, they are governed by the Code of Practice on Covert Surveillance and Property Interference, issued under section 71 of the Regulation of Investigatory Powers Act 2000. However, this does not regulate non-covert use of these cameras, or the use of CCTV by private actors.

The impact of CCTV cameras on the right to privacy was considered by the ECtHR in *Peck v UK* (2003). In this case, the applicant was recorded on CCTV cameras owned by Brentwood City Council walking through the city centre carrying a knife, which he had just used to try to commit suicide. The Council subsequently shared the footage with a television company and the man's undisguised image was broadcast without his consent on a programme watched by 350,000 viewers. In considering the case, the Court found:

> The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life. On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations. (para 59)

The Court further found that the subsequent broadcasting of the event on a television programme without the man's consent or the masking of his image constituted a violation of his right to a private life. The Court added that, although the Council's use of CCTV and the sharing of images with a broadcaster were lawful, in this case the impact on the applicant's privacy was disproportionate. The findings in this case illustrate a legal distinction between the recording and processing of images, in respect of which an individual's privacy rights can be protected, and the mere observing individuals in public spaces, which may not attract any protection.

Interception of communications and surveillance

During the conflict in Northern Ireland, the interception of communications and surveillance were commonly used counter-terrorism techniques. In addition, during the 1970s and 1980s, the UK security services covertly listened to and recorded the telephone conversations of trade union members and left-wing politicians, including members of the government (a process known as 'wiretapping'). In *Malone v Metropolitan Police Commissioner (No 2)* (1979), an English court confirmed that a person had no right not to have his or her telephone tapped by state authorities. There was nothing to make the practice unlawful; therefore, it had to be tolerated. Mr Malone then took his case to Strasbourg, where the ECtHR decided in 1984 that the UK's law was in breach of Article 8 of the ECHR. The Court said that the UK's law did not indicate with sufficient clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities.

The Interception of Communications Act 1985 was passed in order to comply with the ECtHR's judgment in the *Malone* case. This Act made it an offence for anyone to intercept communications sent by post or by means of a public communications system. However, interception remained permissible if it was consented to (eg when someone wishes

to trace offensive telephone calls) or if it was carried out under a warrant issued by the Secretary of State, who must not issue one unless he or she considers it to be necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the UK.

The UK government was forced to introduce further safeguards following the ECtHR's decision in *Halford v UK* (1997). This case concerned the Merseyside Police Authority's decision to intercept the telephone calls of Ms Halford, an Assistant Chief Constable, who had lodged a claim against the authority on the basis that she had been refused promotion because of her gender. The ECtHR found that 'telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8(1)' (para 44). The Court further found that for such interference in individuals' private lives to be considered in accordance with the law, the law must be:

> sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures. (para 49)

The Court held that the Interception of Communications Act 1985 failed to provide such safeguards and hence there had been a violation of Article 8. It recently restated this finding in *Liberty v UK* (2008), which related to the interception of telephone calls between Britain and Ireland in the 1990s. As a result of the *Halford* decision, the Interception of Communications Act 1985 and parts of the Police Act 1977 were replaced by the Regulation of Investigatory Powers Act 2000 (RIPA), which was enacted to try to ensure that the law in this area fully complied with the ECHR and with the newly enacted Human Rights Act 1998.

RIPA permits a wide range of public authorities, including police services and local governments, to make requests for surveillance powers. Depending on the public authority making the request, there can be directed and intrusive surveillance, and the use of covert human intelligence sources, provided these are expressly authorised by designated persons such as the police or the security services (ie those bodies listed in Schedule 1 to the Act). The authorising persons must believe that the authorisation is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the UK (ss 28(3) and 32(3)). Directed and covert surveillance

can also be authorised in the interests of public safety, for the purpose of protecting public health, for the purpose of assessing any tax or for any other purpose specified in an order made by the Secretary of State (s 28(3)). Authorisations of intrusive surveillance granted to the police or customs officers have to be approved by a Surveillance Commissioner (s 36), and appeals against the decisions of that Commissioner can be taken to the Chief Surveillance Commissioner (s 38). RIPA also created an Interception of Communications Commissioner (s 57) who is empowered to monitor whether public authorities are using their surveillance powers legally and responsibly. According to the Annual Report of the Interception of Communications Commissioner, public authorities as a whole submitted 552,500 requests for communications data during 2010. On grounds of national security, the Commissioner declined to reveal what percentage of these requests related to Northern Ireland, and similar restrictions are placed on disclosing the numbers of Foreign Office warrants.

In Northern Ireland, the Office of the First Minister and Deputy First Minister is amongst those who are designated to authorise directed or covert surveillance but not intrusive surveillance (s 31) and there is an Investigatory Powers Commissioner for Northern Ireland to keep this function under review (s 61). The surveillance powers regulated by RIPA were challenged in the case of *Re McE* (2009). This related to covert surveillance by the Police Service of Northern Ireland of conversations between a lawyer and his clients, who were Loyalist paramilitaries. The bugging of the conversations resulted in the lawyer being charged with incitement to murder and perverting the course of justice. In considering the matter, the House of Lords held that RIPA did permit covert surveillance despite the existence of legal professional privilege or statutory rights to consultation with legal representatives. However, such surveillance could be permitted only if the safeguards within RIPA were adhered to and there was no breach of Article 8. Given the severity of intrusion on private legal conversations, the safeguards used had to be those stipulated by section 32 of RIPA.

Privacy, freedom of expression and the media

During 2011, the phone-hacking scandal involving national newspapers and the debates over the use of super-injunctions brought the question of media intrusions on the right to privacy firmly into the public spotlight. Traditionally, in order to preserve press freedom, UK governments have opted to allow the print media to self-regulate, rather than relying on civil or criminal regulation. Individuals who feel that their privacy has been invaded can therefore complain to the Press Complaints Commission, a body dominated by media representatives. If the complaint is upheld, the Commission can censure the newspaper or journalist and may even require its adjudication to be published by the offending paper. However, the Commission has no power to fine an offender or to award damages to a complainant.

Since the entry into force of the Human Rights Act 1998, UK courts have gradually supplemented these self-regulatory protections and established a considerable body of case law on the application of Article 8 to disputes between private actors. As the following paragraphs reveal, the case law to date indicates that when determining whether a private actor has breached an individual's privacy, the courts will ask three questions: do the courts have jurisdiction to intervene; is the published information private; and, if so, is its publication in the public interest?

Do the courts have jurisdiction?

As it is primarily binding only on public bodies, the Human Rights Act 1998 is not directly enforceable against private actors. However, people can now complain about violations of their right to privacy under Article 8 when suing private actors using an existing cause of action such as breach of confidence. When such complaints have been made over the past decade, UK courts have gradually developed an indirect 'horizontal' effect for Article 8 by relying on their own obligation under section 6 of the Human Rights Act to act in a manner that is compatible with Convention rights, and section 12 of the Act specifically requires the courts to balance freedom of expression against the right to privacy. This approach was endorsed by the Court of Appeal of England and Wales in *B and A v C* (2002) and then by the House of Lords in *Campbell v MGN* (2004).

Is the information private?

Traditionally, under the common law, the doctrine of breach of confidence offered some protection against the publication of confidential information. However, UK courts and the ECtHR have gradually extended this to apply to information where individuals have a *reasonable expectation* of privacy. This expectation could arise in relation to the nature of the information, the form in which it is kept, or whether it has been disclosed as part of a confidential relationship.

The reinterpretation of the law of confidence began soon after the Human Rights Act entered into effect, in the case of *Douglas v Hello!* (2001). Michael Douglas and Catherine Zeta-Jones tried to prevent *Hello!* from publishing their wedding photographs, which the two stars had promised instead to give to *OK* magazine. In the English Court of Appeal Sedley LJ said that 'we have reached a point at which it can be said with confidence that the law recognises and will appropriately protect a right of personal privacy' (para 110), but the majority of the court held that here publication should be permitted and refused to continue the interim injunction against *Hello!*. The two stars later successfully claimed damages from *Hello!* for the breach of confidence, but Lindsay J too found that there was not yet a full-blown right to privacy.

The law of confidence was also dramatically employed to protect the right to privacy in *Venables and Thompson v News Group Newspapers Ltd* (2001), where a global injunction was granted to prevent the disclosure of any information which could lead to the identification of the killers of Jamie Bulger after their release from prison. Dame Elizabeth Butler-Sloss held that the information relating to the identification of Venables and Thompson required 'a special quality of protection' as its disclosure could result in 'grave and possibly fatal consequences'. The decision shows that breach of confidence may occur based on the nature of the information alone, rather than the circumstances in which someone acquired it.

It seems, however, that the occurrence of sexual relations per se is not something which has to be treated as confidential. In *Theakston v MGN Ltd* (2002) the judge refused to prevent the publication by the *Sunday People* of photographs of a television presenter engaging in sexual acts in a London brothel. In *B and A v C* (2002), which concerned revelations about the extra-marital affairs of a premiership footballer, the Court of Appeal set out 15 guidelines to help courts strike a balance between privacy and freedom of expression. These stated, for example, that a duty of confidence will arise if the party is in a relationship

in which he 'can reasonably expect his privacy to be protected' and noted that 'the more stable the relationship the greater will be the significance which is attached to it'.

A landmark decision on the protection of private information was delivered by the House of Lords in *Campbell v MGN* (2004), where Lord Nicholls argued that breach of confidence had evolved from relating solely to information that was expressly confidential to include any information a person receives which he or she knows or ought to know is fairly and reasonably to be regarded as confidential. Indeed he suggested that the tort of breach of confidence is now better described as the tort of misuse of private information and that the crucial issue is whether 'the person in question had a reasonable expectation of privacy' (para 21). In the same decision, Lord Hoffmann contended that the tort was now based upon 'the protection of human autonomy and dignity—the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people' (para 51).

This issue was also considered by the ECtHR in *Von Hannover v Germany* (2004), where it found that press photographs of Princess Caroline of Monaco engaging in 'her daily life' had infringed her privacy. In reaching this decision, the Court noted that 'there is ... a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"' (para 50). It also observed that Princess Caroline exercised no official functions and hence the photographs related solely to her private life (para 76). This approach went beyond the approach of the House of Lords in *Campbell v MGN*.

In 2006, in *HRH Prince of Wales v Associated Newspapers Ltd*, the Court of Appeal found that a travel journal handwritten by Prince Charles was a 'paradigm example of a confidential document' as it was obviously private and set out the prince's personal views and impressions (para 35). Although the journal was seen by his staff, they were contractually obliged to keep the journal's contents confidential. Likewise, in *Ash v McKennitt* (2006) an English court prevented the disclosure in a book about to be published by Ms Ash of personal information about Ms McKennitt, a Canadian folk singer. Ash had learned the information in the course of a friendship with McKennitt and whilst being employed by her under a contract containing a confidentiality clause. The court held that McKennitt had a 'legitimate expectation' of protection and respect for her private life, even, on some occasions, in relatively public circumstances (para 52). Even the disclosure of 'anodyne' or 'trivial' information, such as details of the interior of McKennitt's home, could engage Article 8 (para 58).

The concept of a 'reasonable expectation of privacy' was further endorsed by the Court of Appeal in *Browne v Associated Newspapers Ltd* (2007) and by the High Court in *Murray v Express Newspapers Plc* (2007). The latter case concerned unauthorised photographs taken of a child by the *Sunday Express*. In holding that on the facts there was no reasonable expectation of privacy, the court said (in para 36) that it was relevant to consider:

- the attributes of the claimant;
- the nature of the activity in which the claimant was engaged;
- the place at which it was happening;
- the nature and purpose of the intrusion;
- the absence of consent and whether it was known or could be inferred that consent was absent;
- the effect on the claimant; and
- the circumstances in which and the purposes for which the information came into the hands of the publisher.

Courts in Northern Ireland have followed the approach of the English courts. For example, in *Callaghan v Independent News & Media Ltd* (2009), the High Court said that 'the question as to whether there is a reasonable expectation of privacy is an objective question and a question of fact'. The court found that, although under the terms of his release from prison Callaghan could not expect privacy from the police, probation service or prison service, he did retain 'a residuum of privacy', which would need to be balanced against the public interest in publishing information about him. The High Court again applied the same criteria in *Lee v News Group Newspapers Ltd* (2010), which was about the publication of information relating to the personal life of well-known musician Van Morrison. The court found that the case breached the applicant's reasonable expectations as the disclosed information related to private and personal activities and to descriptions of children and the home (para 34).

Is the publication in the public interest?

If the courts find that private information has been disclosed, they then have to determine whether the disclosure was in the public interest. This entails balancing Article 8 protection against the protection of the freedom of expression contained in Article 10 of the ECHR (see Chapter 9). With the entry into force of the Human Rights Act 1998, the right to freedom of

expression became a direct part of UK law, and section 12 of that Act outlines requirements for UK courts to address if they are considering granting remedies, such as injunctions, which would affect freedom of expression. The requirements include having particular regard to the extent to which '(i) the material has, or is about to, become available to the public, or (ii) it is, or would be, in the public interest for the material to be published' and to 'any relevant privacy code'. However, under the Human Rights Act neither Article 8 nor Article 10 has precedence over the other (*Campbell v MGN*, 2004, para 55).

UK courts have engaged in balancing Articles 8 and 10 in numerous cases relating to the publishing of personal information by the media, with differing results. In *Venables and Thompson v News Group Newspapers Ltd and others* (2001), where the disclosure could have had severe consequences for the applicants' security, the court held that: 'This factor not merely rendered the information confidential, but outweighed the freedom of expression that would otherwise have underpinned the right of the press to publish the information.' In *B and A v C* (2002), as noted above, the Court of Appeal, when determining whether media disclosures of the private lives of celebrities are in the public interest, set out guidelines for balancing Articles 8 and 10. These provide that press freedom is itself of public interest, given the role that the media play within society. They further state that courts cannot interfere with press freedom 'where there is no identifiable special public interest in any particular material being published'. However, where there is a clear public interest in publication the Court of Appeal argued that this strengthened the case for publication. As regards public figures, the guidelines state that, although they are entitled to a private life, because of their public position they 'must expect and accept that [their] actions will be more closely scrutinised by the media'. They further state that where public figures have 'courted public attention' they then have 'less ground to object to the intrusion which follows'.

In the landmark *Campbell* case (2004), the majority of the House of Lords found that there was a legitimate public interest in exposing the truth of Ms Campbell's drug addiction as she had previously made public denials about it (paras 24, 58 and 151). In addition, Lord Hope said that the courts have to determine whether publication 'pursues a legitimate aim and whether the benefits that will be achieved by its publication are proportionate to the harm that may be done by the interference with the right to privacy' (para 113).

A few weeks after this ruling, the ECtHR decided the *Von Hannover* case (2004), where it was held that there was no public interest in publishing information on the private life of Princess Caroline because, although she was a public figure, the 'published photos and

accompanying commentaries relate exclusively to details of the applicant's private life' (para 64) and therefore did not 'contribute to any debate of general interest to society', a factor which the court argued should be 'decisive' in balancing Articles 8 and 10 (para 76). In its more recent judgement in *Mosley v UK* (2011) the ECtHR maintained the importance of the distinction between information that informs public debate and information that does not (para 112). In particular, it confirmed that tawdry, lurid or sensational reporting 'does not attract the robust protection of Article 10 afforded to the press' and it stressed that in assessing whether there is a public interest justifying an interference with the right to respect for private life, 'the focus must be on whether the publication is in the interest of the public and not whether the public might be interested in reading it' (para 114). Thus, Article 8 may take precedence over Article 10 where the information being disclosed is private and intimate and will not contribute to public debate.

The importance of weighing the public interest was reiterated by the Court of Appeal of England and Wales in *HRH Prince of Wales v Associated Newspapers Ltd* (2006), and in *Re BBC (Attorney-General's Reference No 3 of 1999*), Lord Phillips said, in the House of Lords, that the test for balancing Articles 8 and 10 had become 'well settled', namely

> whether publication of the material pursues a legitimate aim, and whether the benefits that will be achieved by its publication are proportionate to the harm that may be done by the interference with the right to privacy. (para 23)

In reviewing the facts of the case, Lord Phillips concluded that the goals of disclosure of personal information by the BBC were legitimate as they related to crime prevention, and the methods adopted were proportionate to these aims. In contrast, more recent judgments relating to press disclosures of the details of the extramarital affairs of celebrities have held them not to be in pursuit of legitimate aims and hence not in the public interest (*CTB v News Group Newspapers Ltd*, 2011).

The courts of Northern Ireland have also explored how to balance Article 8 and 10 rights. In *Callaghan v Independent News & Media Ltd* (2009), the High Court distinguished between the public interest 'in relation to the debate as to whether it is right to publish detailed information about sex offenders when they are to be released into the community and if so the extent of that information' and the public interest in publishing unpixelated photographs of particular offenders (para 25). The court found that the publishing of the

photographs might be detrimental to the public interest where it undermined the rehabilitation of offenders, and that therefore the restriction on publishing photographs was proportionate (para 79). Subsequently, in *Lee v News Group Newspapers Ltd* (2010), the High Court held that given the personal nature of the information in this case, concerning the life of Van Morrison, the public did not have a legitimate interest in the claimants' private affairs.

Within the law of both England and Northern Ireland, disclosure of particularly sensitive information, such as the anonymity of rape complaints or the names of children who are party to legal proceedings, is subject to statutory reporting restrictions. However, in order to protect the interests of open justice, these are very limited and specific. In other cases, reporting restrictions are imposed only if it can be demonstrated that the relevant information is private and that its publication is not in the public interest. Where this is proven, the law provides a number of remedies, including injunctions to prevent the publication of the private material and damages to compensate for injury caused by prior publication.

Useful contacts

Big Brother Watch
55 Tufton Street
London SW1P 3QL
email: info@bigbrotherwatch.org.uk
tel: 0207 340 6030
www.bigbrotherwatch.org.uk

Electronic Privacy Information Center
1718 Connecticut Ave
NW Washington, DC 20009
Email: epic-info@epic.org
Tel: +1 202 483 1140
www.epic.org

GeneWatch
60 Lightwood Rd
Buxton SK17 7BB
Email: mail@genewatch.org
Tel: 01298 24300
www.genewatch.org

International Forum for Responsible Media
Email: inforrmeditorial@googlemail.com

inforrm.wordpress.com

JUSTICE
59 Carter Lane
London
EC4V 5AQ
Email: admin@justice.org.uk
Tel: 020 7329 5100
www.justice.org.uk

Liberty
Liberty House
26–30 Strutton Ground
London SW1P 2HR
Email: info@liberty-human-rights.org.uk
tel: 020 7403 3888
https://www.liberty-human-rights.org.uk/?

Privacy International
62 Britton Street
London, EC1M 5UY
tel: 020 3422 4321
email: info@privacy.org
www.privacyinternational.org

Surveillance Studies Network
Email: ssn@surveillance-studies.net
www.surveillance-studies.net