The right to respect for private life: digital challenges, a comparative-law perspective

The United Kingdom

STUDY

EPRS | European Parliamentary Research Service

Comparative Law Library Unit
PE 628.249 – October 2018

EN

THE RIGHT TO RESPECT FOR PRIVATE LIFE: DIGITAL CHALLENGES FROM A COMPARATIVE-LAW PERSPECTIVE

The United Kingdom

STUDY

October 2018

Abstract

This study forms part of a wider-ranging project which seeks to lay the groundwork for comparisons between legal frameworks governing the right to respect for private life in different legal systems, and between the ways in which the systems address the challenges that the 'digital age' poses to the exercise of that right.

The following pages will analyse, with reference to the United Kingdom, the legislation in force, the most relevant case law and the nature of the right to respect for private life. Chapter 2 describes the concept of a right to respect for private life as it is recognised in UK legislation. This section of materials is subdivided into two parts. The first part outlines statutory protection for privacy interests, including the recently enacted Data Protection Act 2018 that gives domestic effect to the General Data Protection Regulations. The rest of chapter 2 discusses the most prominent set of statutory restrictions or qualifications upon the right. Privacy interests are thus revealed to be limited in the interests of national security and the prevention, investigation and detection of crime including crimes connected to the sexual abuse of children and young persons. Particular sets of laws authorise interception, examination and retention of digital online communications. Relevant obligations imposed on ISPs and telecommunications companies are described as are safeguards against unlawful forms of intrusion into these communications. Chapter 3 provides an overview of relevant jurisprudence in privacy related matters. A central focus of this chapter is the relatively recently developed tort of misuse of personal information. An evaluation of the overall state of UK law is offered in chapter 4. Finally, the conclusion identifies some privacy-related issues that are likely to arise in the near future.

AUTOR

This study has been written by **Professor Ian Cram**, Professor of Comparative Constitutional Law, School of Law, Leeds University, at the request of the Comparative Law Library Unit, Directorate-General for Parliamentary Research Services (DG EPRS), General Secretariat of the European Parliament.

CONTACT PERSON

Prof. Dr. Ignacio Díez Parra, Head of the Comparative Law Library Unit.

To contact the Unit, please send an email to: EPRS-ComparativeLaw@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

Translations: DE, ES, FR, IT

This document is available on the internet at: http://www.europarl.europa.eu/thinktank

Manuscript completed in September 2018.

PE 628.249

Print	ISBN 978-92-846-4014-0	DOI:10.2861/53261	QA-06-18-196-EN-C
PDF	ISBN 978-92-846-4016-4	DOI:10.2861/45028	QA-06-18-196-EN-N

Table of contents

List of abbreviations

(Admin)	Administrative Law Division of the High Court
AC	Appeal Cases
All ER	All England Law Reports
anor	another
Ch (D)	Chancery Division (High Court)
CJEU	Court of Justice of the European Union
CTLR	Computer and Telecommunications Law Review
DPA 1998	Data Protection Act 1998
DPA 2018	Data Protection Act 2018
DRIPA 2014	Data Retention and Investigatory Powers Act
ECHR	European Convention on Human Rights
edn	edition
ELRev	European Law Review
EMLR	Entertainment and Media Law Reports
EU Charter	European Union Charter of Fundamental Rights
EWCA Civ	England and Wales Court of Appeal Civil Division
EWCA Crim	England and Wales Criminal Division
EWHC	England and Wales High Court
G-20	International forum of governments and central banks in leading world economies
GCHQ	Government Communications Head Quarters
GDPR	General Data Protection Regulation
HRA	Human Rights Act 1998
IPA	Investigatory Powers Act 2016
IPQ	Intellectual Property Quarterly
LIM	Law and Information Management
MI5	UK domestic counter-intelligence and security agency
MI6	UK foreign intelligence service
NLJ	New Law Journal
NSA	US National Security Agency
p.	page
para	paragraph

QB	Queen's Bench (Division of High Court)
r.	rule
RIPA	Regulation of Investigatory Powers Act 2000
s.	section
ss.	sections
UKHL	United Kingdom House of Lords (Court)
UKIPTrib	United Kingdom Investigatory Powers Tribunal
UKSC	United Kingdom Supreme Court
WLR	Weekly Law Reports

Executive summary

For many years the United Kingdom did not have a direct remedy for infringement of privacy interests. Instead, litigants wishing to assert a privacy type interest in the face of either (i) physical intrusion onto land or (ii) non-consensual disclosure of information to third parties were obliged to frame their claims in terms of pre-existing remedies for *inter alia* trespass, breach of confidence (in equity), nuisance, malicious falsehood and copyright.

The UK Parliament assumed a more active role in regulating by statute forms of physical harassment in the Protection from Harassment Act 1997. This was passed after the tabloid/paparazzi treatment of Princess Diana that culminated in her death in a motoring accident whilst fleeing the attention of photographers in Paris.

Shortly afterwards the passing into law of the Human Rights Act 1998 enabled the principled recognition of individual privacy interests. From the 1998 Act's commencement in October 2000, individuals were able to invoke Article 8 of the European Convention on Human Rights (and associated Strasbourg caselaw) directly against public authorities. Where the allegation of privacy intrusion was made against a non-public body (such as a privately-owned media organisation), individuals could not make Article 8 ECHR type claims directly against the non-public body. Instead, claimants were (and are to this day) required to serve proceedings under a pre-existing form of civil action against the publisher (such as malicious falsehood, breach of confidence or misuse of personal information). Only then will the court (as a public authority itself) allow the remedy in question to be reinterpreted in light of the Strasbourg jurisprudence on Article 8 (often alongside other relevant Convention Articles such as Article 10 – the right to freedom of expression).

Problems concerning the physical harassment of individuals via a course of conduct are now largely regulated by the Protection from Harassment Act 1997. The jurisprudence to emerge under this Act has determined that speech can be conduct. It follows that dissemination via *Twitter* or *Facebook* of tweets/posts that could foreseeably cause a person distress and alarm might constitute harassment for the purposes of the 1997 Act. Needless to say some commentators already envisage that the 1997 Act will at some stage be deployed against abusive online speakers.

A range of domestic statutes confer discrete degrees of protection for privacy interests in domestic law. These include statutes which criminalise voyeurism, the phenomenon of 'revenge porn', computer hacking, publication of the identities of children and other specified persons who appear before the courts as defendants, witnesses and complainants. The major recent statutory reform is however the Data Protection Act 2018 that seeks to give domestic effect to the General Data Protection Regulations. The enforcement mechanisms include powers to impose increased financial penalties on companies that violate data protection principles. In July 2018, *Facebook* was found to have broken principles relating to both data security and informed user consent. The relatively small fine imposed by the Information Commissioner on the social media giant is explained by the fact that the 2018 Act was not in force when the breaches were committed by *Facebook*. Recent evidence concerning the sorts of use to which the improperly disclosed data has been put indicates that political organisations competing for electoral support are as interested in harvesting users' data as commercial organisations seeking to tap into new consumer markets.

Privacy is of course a qualified right in liberal democratic systems of government. It is recognised that the right *must* give way in the face of competing and compelling interests in protecting national security and the prevention and detection of crime. At the same time, it is important that the powers accorded to state security and policing agencies are exercised

proportionately and overseen by elected representatives. A valuable check against the misuse of such powers of surveillance is provided by the requirement of prior judicial approval. Unfortunately as recent litigation has made clear, a recurring defect in the UK legislative framework has been failure to require prior judicial approval for certain kinds of surveillance warrant giving rise to the grave criticism from the UK judiciary that state security agencies have been acting outside the rule of law. As the respective rulings in cases such as *Privacy International* (2016), *R (on the application of Liberty v Secretary of State for Home Department & Secretary of State for the Foreign and Commonwealth Office* (2018) and *Secretary of State for the Home Department v Davis, Watson and others* (2018) all make clear, the 2014 DRIPA and 2016 IPA legislation have failed to meet the standards of independent oversight required under either EU and/or ECHR law. At the time of writing the UK Government has promised detailed amendments to IPA 2016 by the autumn of 2018 to meet current concerns. IPA 2016 also mandates the indiscriminate retention of meta data by telecommunications companies for access by a range of bodies including financial services regulators and local authorities whose remit does not extend to state security or the prevention/detection of crime. This anomaly was highlighted by the court in *Watson* and will need to be addressed in the near future.

An increasingly important aspect of privacy is that protected under Article 17 of GDPR and the so-called 'right to be forgotten' recognised by the CJEU in *Google Spain*. The UK Courts are beginning to determine cases brought under these new laws and are likely to be asked to make significant rulings in the future. One prominent concern is that, facing the prospect of a huge fine for failing to comply with a de-listing request, a search engine or other digital intermediary is incentivised to close down legitimate expression in the public interest in the fact of powerful individuals/companies who seek to limit access to critical commentary and analysis of their previous activites, including criminal convictions administered in open court and reported contemporaneously in the media.

Other laws authorise the violation of individual or corporate privacy interests. These include laws aimed at the prevention of harm to children and young persons caused by the possession and making of child pornography and child sex abuse manuals. In the case of the Digital Economy Act 2017, the statutory objective is to prevent young persons accessing sexually explicit materials depicting adult sex online. The regulatory body is entitled to require such websites to adopt mandatory age verification controls. Moreover ISPs and website operators may be obliged to disclose their users' personal data in certain circumstances.

At common law the remedy of misuse of personal information has emerged in recent years as one of the most valuable forms of action to protect individuals from unwarranted disclosures concerning their private lives. This remedy has grown out of the equitable action for breach of confidence in the *post* Human Rights Act era.

To succeed in an action for misuse of personal information, a claimant must show that he/she has a reasonable expectation of privacy in the first place and then that the balance of Article 8 and Article 10 ECHR interests favours the privacy claim. This is the test from *Campbell v MGN* – a ruling of the House of Lords in 2004. *Campbell* follows ECHR jurisprudence in holding that there is no presumptive priority between either Article. What can be put on each side of the balance in any given case is inevitably highly fact specific.

An action for misuse of personal information is often accompanied by an application for a an interim injunction to prevent media organisations (including the defendant publisher) from publishing the allegedly private matter in advance of a full hearing on the merits of the misuse of personal information suit. The issuing of such injunctions is governed by s.12 of the Human Rights Act 1998.

Recent developments in the tort of misuse of personal information in cases such as *Sir Cliff Richard OBE v BBC and Chief Constable of South Yorkshire* (2018) suggest that the outer boundaries of this privacy-protecting tort may be expanding. In *Sir Cliff Richard OBE* the High Court held that, as a matter of general principle, suspects under investigation by the police were entitled to remain anonymous and the media was also prevented from reporting the fact of a search at the suspect's property. This is a novel development in domestic law.

I. Introduction

For many years, the UK did not possess a privacy law in name. Accordingly, there could be no action for violation of privacy *per se*. Instead, those alleging (i) some form of physical intrusion into land that they owned or lawfully occupied or (ii) wrongful disclosure of personal information to third parties were required to base their claims upon pre-existing remedies that acted in effect as a privacy surrogate. Such remedies included civil actions for malicious falsehood, trespass to land, private nuisance and the law of confidence. Injunctions might also be issued to prevent an ongoing violation of the claimant's rights.

Following concerns about the conduct of certain media publications, the UK Parliament passed the Protection from Harassment Act 1997 which remains on the statute book today. This statute allows for claims by persons who are the victims of a course of conduct[1] that a reasonable person would consider to constitute harassment.[2] In the continuing absence of a general statutory right to privacy, the judges in the higher courts have also developed new civil law remedies to protect privacy interests in with the UK's obligations under the European Convention on Human Rights.

The principal protection in this regard is the tortious action for misuse of personal information that was effectively created by the House of Lords in the case of *Campbell v Mirror Group Newspapers Ltd*.[3] The precise contours of the new tort have become clearer with subsequent rulings to the point in 2018 where, following *Sir Cliff Richard OBE v BBC and Chief Constable of South Yorkshire*, there is as a matter of general principle a reasonable expectation of privacy on the part of persons who are suspects in police investigations but remain at the time of reporting unarrested.

In respect of digitally held information, Data Protection Act 1998 sought to give individual data 'subjects' a measure of control over the data that was held about them by those who collect such information, including businesses. Consequently, rights of access, correction and erasure in respect of inaccurate data were recognised by the 1998 Act enforceable by natural persons against data controllers who determine the purposes and means by which the information is to be processed. UK law has since been updated by the Data Protection Act 2018 Act. This latest Act aims to make UK law ready for the challenges presently posed by the digital era when vast amounts of personal information are collected, stored and disseminated online. The 2018 Act is explicitly intended to be compliant with the General Data Protection Regulation (EU) 2016/679. In July 2018 *Facebook* was found by the UK Information Commissioner to have breached data protection principles in 2014 and 2015 (and thus dealt with under the 1998 Act) regarding (i) the safeguarding of users' information and (ii) transparency obligations to users as to how their personal data was to be passed on to others.

State interests in national security and the effective investigation and detection of crime have long necessitated the surveillance of persons and organisations both within and beyond national borders. The Snowden revelations in 2013 established that UK state security and intelligence agencies had been engaged and were continuing to engage in unauthorised surveillance and data collection of citizens' digital communications through programmes such as *Tempora*. Data thus obtained was then shared with the US National Security Agency. The

---

1 A course of conduct requires there to be at least two occasions where the conduct complained of has occurred, s.7(3) 1997 Act. 'Conduct' can include speech (s.7(4)).

2 Harassment is otherwise not defined in the Act.

3 [2004] UKHL 22.

revelations also showed that GCHQ at Cheltenham UK monitored foreign politicians' phone conversations whilst attending a G-20 summit in London in 2009. Snowden's disclosures also suggested that GCHQ was responsible for a cyberattack on *Belgacom* a Belgian telecommunications company whose clients include the European Parliament. The attack was apparently intended to target specific employees to enable UK intelligence agencies to have access to Belgacom's infrastructure.[4]

[4] http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

II. The concept of right to respect for private life in the British legislation

II.1. Introduction

The discussion below is divided into two parts. Statutes in domestic law that confer a measure of protection for individual and corporate and other organisations' privacy interests against physical intrusion or disclosure are described in II.1.1. Next a section of legislative provisions authorising interference with individual and corporate privacy interests is outlined. Attention here is also devoted to any privacy safeguards that have been built into the legislation. In each case, the jurisprudence accompanying the relevant provisions is set out in Part III. In each part it will be seen that discrete privacy interests of persons and organisations are capable of being infringed in distinct ways by either digital (e.g. accessing private electronic communications) or non-digital means (e.g. physical intrusion). A range of civil law remedies and criminal penalties attach to intrusive conduct. Sometimes, the legislation makes no differentiation between the two types of infringement. Some UK legislation focuses exclusively upon digital infringements of privacy (as tends to be the case with more recent statutes).

II.1.1. Protection from Harassment Act 1997

The Protection from Harassment Act 1997[5] creates a set of civil law remedies for persons who are the victims of a 'course of conduct'[6] by another that a reasonable person would consider to constitute harassment.[7] Damages may be awarded where the claimant has suffered anxiety and/or financial loss. An ancillary criminal law remedy provided under the 1997 Act permits a court to fine or imprison a person found guilty of harassment. Regardless of whether a person is convicted of harassment, a restraining order can be made by the Court against a defendant.[8] Harassment may occur through physical conduct, for example stalking. It may also extend to publishing information about a person or repeated communication with a person. This is because 'conduct' is expressly defined to include speech in s.7(4) and the courts read this provision as requiring an interpretation that is consistent with the right to respect for private life under Article 8 of the European Convention on Human Rights. Commentators note that the 1997 Act is 'becoming an increasingly important tool for those seeking to protect their privacy against intrusion by the media and private persons.'[9] The jurisprudence on these matters is dealt in greater detail below. Defences are available under the Act for those who can show that the conduct in question occurred (a) in the pursuit of preventing or detecting crime; (b) under an enactment or rule of law; or (c) in circumstances that render the conduct reasonable.[10]

---

5 https://www.legislation.gov.uk/ukpga/1997/40/contents.

6 A course of conduct requires there to be at least two occasions where the conduct complained of has occurred, s.7(3) 1997 Act. 'Conduct' can include speech (s.7(4)).

7 Harassment is otherwise not defined in the Act.

8 S.5 & 5A 1997 Act.

9 Tugendhat & Christie *The Law of Privacy and the Media* (3rd edn) (2016, OUP, Oxford) at 269.

10 S.1(3).

II.1.2. Criminal Justice and Police Act 2001 s.42 'physical harassment of another inside a dwelling place'[11]

Section 42 gives police officers the power to give directions to persons outside dwelling places to prevent the harassment, alarm or distress of persons inside that place. It is an offence in breach of such a direction for someone outside a dwelling place to persuade or represent to an individual inside the dwelling place that the individual should (i) do something that his not under any obligation so to do, or (ii) not do something that he is entitled lawfully to do. Liability occurs where both (i) the person intends to harass, alarm or distress the individual or is aware that his presence is likely to have one of these effects; and (ii) harassment, alarm or distress is caused or s likely to be caused by the person's conduct.

II.1.3. Sexual Offences Act 2003 s.67 – 'voyeurism'[12]

This makes it an offence to observe (whether with operating equipment or not) another person doing a private act for the purposes of the observer's sexual gratification. Liability only exists where the observer knows that the observed person does not consent to being observed.

II.1.4. Criminal Justice and Courts Act 2015 s.33 – 'Revenge Porn'[13]

It is an offence to disclose a private sexual photograph or film to a person other than the photographed/filmed person without the latter's consent for the purpose of causing distress.[14] This section aims to protect the privacy of former sexual partners who find that filmed/photographed images of themselves and of a sexual nature are being disseminated without their consent to third parties, often out of a desire to humiliate or embarrass the former partner.

Defences exist where (i) it is reasonably believed that disclosure is necessary for the purposes of the investigation, prevention or detection of crime;[15] or it is disclosure is made in the course of, or with a view to, the publication of journalistic material and it is reasonably believed that publication is in the public interest.[16]

II.1.5. Data Protection Act 2018[17]

The 2018 Act repeals the previous Data Protection Act 1998 and seeks to make UK law fit for the challenges posed by the digital era when vast amounts of personal information are collected, stored and disseminated online. The 2018 Act is intended to be compliant with the General Data Protection Regulation (EU) 2016/679 (hereafter GDPR). Data must be processed by data controllers according to a set of data protection principles.[18] These are

1) Processing be lawful and fair
2) Purposes of processing be specified, explicit and legitimate
3) Personal data be adequate, relevant and not excessive
4 Personal data be accurate and kept up to date

---

11 http://www.legislation.gov.uk/ukpga/2001/16/contents.

12 https://www.legislation.gov.uk/ukpga/2003/42/contents.

13 http://www.legislation.gov.uk/ukpga/2015/2/contents/enacted.

14 S.33(1).

15 2015 Act, s.33(3).

16 2015 Act, s.33(4).

17 http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

18 Data Protection Act 2018, ss.34-40.

5) Personal data be kept for no longer than is necessary
6) Personal data be processed in a secure manner

It is to be noted here that the 2018 Act exercises a number of derogations/discretions available to national governments within the GDPR (such as what counts as a public authority for the purposes of the new law; the age at which children can consent to their personal data being processed; the circumstances in which personal data may be processed without explicit consent e.g. data concerned with criminal conviction, the pricing of risk in financial services, anti-doping programmes in sport). The 2018 Act also permits the continued processing of personal data without explicit personal consent where there is a substantial public interest. The example is given of the inquiry in 2009 into the 1989 Hillsborough Stadium disaster when 96 football supporters died. The inquiry needed access to personal data held by individuals and organisations in order to establish the truth surrounding the disaster.

The UK Government intends that the 2018 legislation will be consistent with the Council of Europe's Convention for the Protection of Individuals with Regard to the Processing of Personal Data (modernised Convention 108) adopted by the Committee of Ministers on May 18, 2018. It is the Government's stated aim that when the UK leaves the European Union, the GDPR will be effectively incorporated into UK law via the UK Parliament's Withdrawal legislation. The 2018 Act adopts the enhanced rights of data subjects provided in the GDPR (such as more explicit consent for personal data processing, stronger rights to be informed about the data that is held about them, to object to direct marketing and profiling for public interest purposes and more direct means of obtaining rectification for inaccurate data).

Data held and processed by the police and other criminal justice agencies for the purposes of the investigation, prevention, detection and prosecution of crime is not covered by the GDPR but by Law Enforcement Directive (EU) 2016/680. This is incorporated into UK by Part 3 of the 2018 Act.

Personal data concerning national security is regulated by Part 4 of the 2018 Act and reflects Council of Europe modernised Convention 108. This section of the legislation contains a set of exemptions from data subjects' rights for the purposes of safeguarding national security.

The enforcement of the 2018 Act is entrusted to the Information Commissioner. He/she has powers to investigate alleged breaches of the Act and fine data holders up to a maximum of £17 million or 4% of turnover in the most serious cases. For breaches committed before the 2018 Act came into force, the maximum fine is £500,000.

II.1.6. Contempt of Court Act 1981[19] and associated administration of justice provisions protecting individual privacy interests

Notwithstanding a commitment in UK law to the principle of open justice whereby judicial proceedings are usually heard in public (and thus freely reportable in the media), it is recognised that exceptionally a countervailing interest in keeping certain matters out of the public domain may be justified. One of the exceptional categories relates to the respective privacy interests in criminal proceedings of victims and witnesses and those of children and young persons more generally. In summary, protection for privacy interests includes automatic reporting restrictions on identification when children and young persons appear in Youth Court proceedings (this includes when the child/young person appears as a defendant).[20]

[19] https://www.legislation.gov.uk/ukpga/1981/49.

[20] Children and Young Persons Act 1933, s.49. The protection ceases when the young person reaches the age of 18 years.

When a child/young person appears in adult court proceedings, the open justice principle applies unless the judge uses his/her discretionary powers under statute to issue a reporting restriction.[21] On the civil law side, family proceedings (which may also involve children and young persons) are typically held in private. Media representatives are however allowed to attend proceedings but cannot report aspects of proceedings beyond a bare outline account.[22] Proceedings brought under Mental Health legislation are also not publishable as a general rule.[23]

The importance that is attached to encouraging witnesses to come forward in criminal proceedings means that adult witnesses may be the beneficiaries of non-identification orders under s.11 of the Contempt of Court Act 1981. According to the established case law, this power is available where the court reasonably believes that anonymity is necessary to serve the ends of justice.[24] Rape and other serious sexual assault complainants also enjoy lifelong anonymity once they have made a formal complaint to investigating authorities.[25] Anonymity lasts for the complainant's lifetime regardless of whether any person is subsequently convicted of an offence arising out of the matters complained of.

II.1.7. Rehabilitation of Offenders Act 1974[26] – non disclosure of past criminal record

A degree of privacy is conferred on persons who have been convicted of criminal offences. Thus persons need not disclose their previous 'spent' criminal convictions when applying for employment, insurance cover or housing provided certain conditions are satisfied. A conviction becomes 'spent' after a specified period of time that correlates to the length of sentence imposed upon the prisoner. Thus for persons sentenced to a period of imprisonment for between 30 months and 4 years, the conviction becomes spent after 7 years from the end of the sentence. By contrast for persons sentenced to a period of imprisonment of between 6 and 30 months, the conviction becomes spent 2 years after the end of the sentence. For persons convicted to a period of custody in excess of 4 years, the conviction is never spent and must always be disclosed. Exempted professions include medical, dentist and legal professionals, chartered accountants, chemists and Jobs that involve contact with children and young persons. For job applicants seeking employment in these fields full disclosure of any previous convictions must be made at the time of application. It is not defamatory in English Law for the media (whether online or offline) to refer to the fact of a spent conviction (even though the convicted person's record has been effectively been wiped clean by the 1974 Act and the subsequent reference to the spent conviction causes reputational damage to the person). However, if the convicted person can show that publication in the media was made maliciously and was not in the public interest, the media lose its protection from the ordinary application of defamation law and may be sued by the named individual.

The acknowledgment by the CJEU of a 'right to be forgotten' in *Google Spain*[27] in 2014 alongside the broader right to erasure of certain personal data held by data controllers under

---

21 Youth Justice and Crminal Evidence Act 1999, s.45A. The basis of the protection is to shield young persons from the trauma of publicity and, in the case of convicted young persons, to facilitate their rehabilitation.

22 Administration of Justice Act 1960, s.12; Family Procedure Rules 2010 SI 2010/2955 r.27.10.

23 Administration of Justice Act 1960.s.12.

24 *AG v Leveller* [1979] AC 440.

25 Sexual Offences (Amendment) Act 1992, s.1.

26 https://www.legislation.gov.uk/ukpga/1974/53.

27 Case C-131/12.

GDPR may mean that in future that some convicted criminals are able to remove details of historic criminal convictions from search engine results. This is discussed in more detail below.

II.1.8. Computer Misuse Act 1990[28] – computer hacking

Unauthorised access to another's computer system is a specific offence in UK law. Section 1 of the Computer Misuse Act 1990. The offence can be comitted from outside the United Kingdom.[29]

II.2. Statutory interferences with privacy

A number of statutes authorise public bodies to interfere with individual and corporate privacy interests (including those of media organisations) for purposes that include the prevention and detection of (i) crime and (ii) terrorism. Some examples were noted above in relation to exemptions from the Data Protection Act 2018 (and associated GDPR). Inasfar as these provisions require media bodies and journalists to disclose materials and sources of information, they raise difficult Article 10 ECHR issues concerning the ability to engage in newsgathering that is vital for the maintenance of informed democratic debate. Other provisions criminalise the possession of certain kinds of material whether held in digital or hard copy format. These include the holding of 'extreme pornography' and indecent images and pseudo-images of children, as well as written/online manuals that facilitate child sexual abuse. Since the revelations by Edward Snowden of mass surveillance programmes by governments (including the UK Government) that were lacking a clear basis in law and largely unacknowledged in the public domain, a tranche of new legislation has been brought forward by the UK Parliament and, in some important aspects, already been found to be deficient by the courts.

II.2.1. Investigatory Powers Act 2016[30]

When Edward Snowden disclosed files indicating that the UK government (along with others) had engaged in mass surveillance without a clear basis in law or endorsement from the legislature, it became clear that the existing domestic legal framework had not kept pace with technological developments and surveillance practice.[31]

In what follows selected key provisions of the legislation are set out. The 2016 Act employs concepts such as 'targeted' material, 'bulk' material, 'contents' data and 'communications' data. These terms are explained below.

II.2.1.1 Interception of targeted data

The statute enables specified intelligence agencies and law enforcement bodies to apply for warrants enabling targeted interception of specific persons' digital devices such as phones, laptops and PCs. A distinction is made in the Act between communications data and the content of communications. 'Content' refers to the actual message contained in the communication. 'Communications' data on the other hand refers to non-content material such as the sender/recipient of a message, the time, and duration of a communication, type or method of communication, the system through which it is carried and the location of the

---

28 https://www.legislation.gov.uk/ukpga/1990/18/contents.

29 Computer Misuse Act 1990, s.4(4)(A).

30 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

31 For contrasting views on the merits of Snowden's actions, see G Greenwald, *No Place to Hide Edward Snowden, the NSA and the Surveillance State* (2015, Penguin Books, London) and E Epstein, *How America Lost its Secrets*: *Edward Snowden, The Man and the Theft* (2017, Knopf Publishing Group, New York).

system. Warrants seeking to intercept the contents of a targeted digital device are the most intrusive forms of surveillance and, accordingly, are subject to the most stringent privacy protections found in the Act. The judicial commissioners appointed under the Act may authorise such a warrant where necessary and proportionate for the purposes of national security, preventing/detecting serious crime, serious damage to UK economic interests (in the context of national security and where the threat comes from persons outside the UK).[32] In deciding whether to grant the authorisation, a judge must be satisfied on grounds of necessity and proportionality that the warrant should be granted, bearing in mind the privacy interests of affected persons.

II.2.1.2 Retention by telecommunications companies of communications data

Part IV of IPA 2016 also empowers inter alia certain public agencies/authorities to require a telecommunications company by means of retention notice to retain records of an individual's internet use for up to 12 months, including senders/recipients of communications, time and duration of a communication and the websites that the person has accessed but not the content of communications.[33] Safeguards include the fact that judicial authorisation for such retention must be granted on the basis that the retention is necessary and proportionate for the purposes set out in s.87 of the 2016 Act. If authorisation is not granted, the Secretary of State can effectively re-apply to Investigatory Powers Commissioner for the retention notice to be authorised.

The powers conferred on government ministers to require that private telecommunications companies retain records of persons' communications data including internet sites visited, location details and personal contacts were adjudged by the High Court to be unlawful in April 2018 in *R (on the application of Liberty) v Home Secretary and Foreign Secretary*.[34] The ruling held that since the retained data could be accessed by a range of bodies including local authorities and financial regulators, the powers could not be said to be limited to the purpose of the prevention or detection of 'serious crime' or 'terrorism'. These bodies' access was not subject to prior judicial authorisation or independent review.[35] As such it was in violation of EU law. The UK Government has been given until the beginning of November 2018 to amend Part IV of the 2016 Act.

This latest setback for the UK Government came after the ruling in *Watson* when the predecessor legislation (s.1 of Data Retention and Investigatory Powers Act 2014) was held by the Court of Appeal to violate EU law on the same grounds.[36] In *Watson* the indiscriminate retention of 'communications data' (revealing not the content of what was spoken/texted but rather who spoke to whom, for how long, at what time and on what forum) were inconsistent with EU law in the absence of sufficient safeguards including prior judicial/independent authorisation. *Watson* itself followed on from the case of *Digital Rights Ireland* before the CJEU which upheld a challenge to the EU's Data Retention Directive.[37] The latter's requirement to store customers' billing data (including identity of speaker, location of mobile phone calls) for between 6-24 months in order to assist in the investigation and detection of serious crime by

---

32 IPA 2016, s.20.

33 This was the result of a successful Oppostion amendment tabled during parliamentary proceedings.

34 [2018] EWHC 975 (Admin).

35 Article 8(3) EU Charter of Fundamental Rights.

36 *Secretary of State for Home Dept v Davis, Watson and others* [2018] EWCA Civ 700.

37 Joined Cases C-293/12 and C-594/12.

the police and security services was deemed invalid as a disproportionate interference with EU citizens' privacy entitlements.

II.2.1.3 Interception and retention warrants in respect of bulk (overseas) data

'Bulk' data refers in the main to external, overseas communications. The interception, acquisition of bulk data and equipment interference are now regulated in Part 6 of the 2016 Act.

Intelligence agencies are given additional powers to engage in 'bulk' data surveillance that are directed at a group or class of persons without specific targeting. This type of surveillance may reveal both contents of communications as well as communications data. Applications are made to the Secretary of State who must consider six conditions in s.138 of the 2016 Act to have been satisfied by the application. These are:

1. the purpose of the warrant is either (i) to intercept overseas-related communications; and/or (ii) to obtain secondary data from such communications; and
2. it is in the interests of national security, the prevention or detection of serious crime, or the economic well-being of the UK (where those interests are also relevant to national security); and
3. the conduct authorised is proportionate to the operational objective to which the conduct relates; and
4. the specified operational purposes for which the warrant is sought is a purpose for which the examination of the intercepted content or secondary data is or may be necessary; and
5. the Secretary of State considers that satisfactory arrangements are in force in relation to the examination, retention and disclosure; and
6. where a telecommunications operator outside the UK is likely to be required to provide assistance, the Secretary of State has complied with his/her mandatory duties of consultation with that telecommunications operator; and

Where the Secretary of State considers that each of 1-6 above have been satisfied, the warrant must then be approved by a Judicial Commissioner who reviews the Secretary of State's conclusions on points 1-6. In deciding whether to approve the warrant, the Judicial Commissioner applies the principles employed in judicial review hearings (e.g. unreasonableness, irrelevant considerations, improper purposes etc.) When carrying out this function, the Judicial Commissioner is required to act with 'a sufficient degree of care' to ensure compliance with the privacy entitlements of those subject to the intrusion.[38]

Bulk interception warrants are limited to interception of the contents of communications sent or received by individuals outside the UK and/or data that enables the identification of senders and recipients. Warrants are only permitted under this part of the Act if a judicial authority is satisfied that they are necessary in the interests of (I) national security; (ii) the prevention or detection of serious crime; and (iii) the economic well-being of the United Kingdom.

II.2.1.4 Targeted warrants – urgent cases

In the case of targeted interception warrants, the issuing authority[39] may forgo the need for prior judicial approval and execute a warrant provided the issuer notifies a Judicial

[38] IPA 2016, s.140(2).

[39] IPA 2016, s.18. The list of authorising persons includes the heads of intelligence services and chiefs of police.

Commissioner that the warrant has been issued. The Judicial Commissioner then has three working days from the date of issue to approve the warrant. If approval is refused, the warrant ceases to have effect.[40] Moreover, the Judicial Commissioner 'may direct that any material obtained under the warrant is destroyed'.[41] In cases where approval is given, the Judicial Commissioner may impose conditions on the retention and subsequent use of material obtained.[42] Urgent authorisations lapse after the fifth working day after issue unless renewed.[43]

II.2.1.5 Additional safeguards for targeted warrants – MPs, legally privileged items confidential journalistic material

Certain categories of targeted material are regarded as raising especially strong privacy concerns. The 2016 Act purports to confer greater protections for these categories of data. Thus, in the case of targeted interception warrants whose purpose is to examine the contents of communications between MPs (including Members of the Scottish Parliaments, Members of the Northern Ireland Assembly, Members of the Welsh Assembly, Members of the European Parliament), before the Secretary of State decides whether to issue the warrant, he/she must first consult the Prime Minister.[44]

In respect of legally privileged communications between lawyers and clients, s.27 of IPA requires the issuing authority to have regard to the public interest and the confidentiality of the items subject to legal privilege. The authority must

> consider that there are exceptional and compelling circumstances that it make it necessary to authorise or require the interception or … the selection for examination of items subject to legal privilege.[45]

Where there are other means by which the information could reasonably obtained, it will not be possible to establish the necessity of authorising interception. If the warrant is sought for the purposes of the prevention and detection of serious crime, then it must be shown that obtaining the information is necessary for preventing death or significant injury.[46]

Journalists' materials and sources are also accorded especial protection under the Act. Where an authorising person is considering issuing a warrant that will enable the interception and examination of material including confidential material created or acquired for the purpose of journalism,[47] they may only do so if they consider that the safeguarding arrangements relating to retention, disclosure and destruction of any confidential material are in place.[48]

---

40 IPA 2016, s.24.

41 IPA 2016, s.25(3).

42 IPA 2016, s.25(b), (c).

43 IPA 2016, s.32(2).Non-urgent targeted warrants approved in advance by a Judicial Commissioner endure for six months from the day of issue.

44 IPA 2016, s.26.

45 IPA 2016, s.27 and see further analysis at p.34 below.

46 IPA 2016, s.27(6).

47 IPA 2016, s.264.

48 IPA 2016, ss.28-29.

II.2.2. Police and Criminal Evidence Act 1984[49]

The 1984 Act authorises police officers to search persons and property under specified circumstances for the purposes of the prevention and detection of crime and with certain safeguards for those who are subject to the exercise of search powers.[50] In addition, powers to take samples (by force if necessary in the case of non-intimate samples such as non-pubic hair) from arrested persons for the purposes of furthering the investigation are conferred by the Act. These allow the police to acquire a DNA profile of arrested persons. Where an arrested person is subsequently convicted of an offence, the DNA profile will be held on a national database indefinitely without any infringement of the person's Article 8 ECHR rights. Where a person is acquitted or otherwise not convicted of the offence in respect of which the sample was taken, the profile may be held for three years, extendable by a further two years where the person has a previous conviction for a recordable offence.[51]

Further provisions exist in Part 1 in relation to requiring journalists to disclose their materials to investigating officers. Safeguards include the requirement to obtain prior judicial consent.

II.2.3. Contempt of Court Act 1981[52] s.10 'journalists' sources'

This provision has considerable significance for the privacy interests of journalists and media organisations. It offers a measure of protection in respect of the confidentiality of sources of information and, so doing, helps to maintain a flow of information into the public domain. The latter plays an important role in facilitating informed scrutiny of politicians and public bodies. Section.10 creates a rebuttable presumption that a journalist (or other person) will not normally have to disclose a source used in the publication of an article, blog or book. The party seeking disclosure of the source's identity will have to satisfy the court that disclosure is *necessary* in the interests of 'justice' or 'national security' or 'the prevention of crime or disorder.' UK case law in this area has sought to take account of Strasbourg Article 10 ECHR jurisprudence. Where, as will be likely, journalists' materials are held in digital form, access to such materials may well be made under the Investigatory Powers Act 2016 (see above).

II.2.4. Criminal Justice and Immigration Act 2008[53], s.63 'extreme pornography'

It is an offence for a person to be in possession of an image that portrays in 'an explicit and realistic way' acts which 'threaten a person's life, acts which result in or are likely to result in serious injury to a person's anus, breasts or genitals, bestiality or necrophilia.'[54]

---

49 https://www.legislation.gov.uk/ukpga/1984/60/contents.

50 See thus Parts 1 & 2 of the 1984 Act.

51 Protection of Freedoms Act 2012, amending the Police and Criminal Evidence Act 1984 at http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted. For background see *Marper v UK* [2009] 48 EHRR 50.

52 https://www.legislation.gov.uk/ukpga/1981/49.

53 https://www.legislation.gov.uk/ukpga/2008/4.

54 2008 Act, s.63(7).

II.2.5. Protection of Children Act 1978[55], Criminal Justice Act 1988[56] – making indecent images of children, possession of indecent photographs of a child

The Protection of Children Act 1978 – a pre-digital, pre-Internet era statute – was updated in 1994 to make it a criminal offence to make an indecent image of a child.[57] The Criminal Justice Act 1988 made it an offence to possess an indecent image of a child.[58] Both provisions are aimed at stemming the (largely digital) traffic in indecent images of children that is connected with the sexual grooming of other children.

II.2.6. Serious Crime Act 2015[59] – possession of a child sex abuse manual

Section 69(1) makes it an offence to be in possession of 'any item that contains advice or guidance about abusing children sexually'. An 'item' includes anything 'in which information of any description is recorded.'[60] Defences exist where the accused can prove that he/she (i) had a legitimate reason for being in possession of such an item; or (ii) had not read/viewed the item; or (iii) did not know and had no reason to suspect that the item contained advice or guidance about abusing children sexually; or (iv) that it was sent to the accused without being requested by him/her or someone acting on his/her behalf. In respect of (iv) the accused must also prove that he/she did not keep the item for an unreasonable time.

II.2.7. Digital Economy Act 2017[61] – preventing young persons' access to pornographic material

One of the main purposes of the legislation is to stop young persons accessing online pornographic materials. Part 3 of the 2017 Act thus requires all websites carrying sexually explicit materials to adopt mandatory age-verification controls on pornographic websites. 'Pornographic' is given a broad definition in section 15 of the Act. Regulators are given broad powers to ensure that the law is complied with. These include financial penalties and in the worst cases a total block on user access. Privacy issues in respect of those adults lawfully accessing the site who must provide age verification data via credit card details or other identifying personal data. In the event of insecure systems of data processing by the website operators, lawful users' data may be vulnerable to hacking by others

The regulatory body set up under the Act may request both ISPs and website operators to disclose users' personal data.[62] In cases of non-compliance with a notice from the regulatory body, an ISP may be obliged to deny access to the website to all persons in the UK.

---

55 https://www.legislation.gov.uk/ukpga/1978/37.

56 https://www.legislation.gov.uk/ukpga/1988/33/contents.

57 The original version of the offence had referred only to the 'taking' of an indecent photograph.

58 1988 Act s.160.

59 http://www.legislation.gov.uk/ukpga/2015/9/contents/enacted.

60 2015 Act s.69(8).

61 http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted.

62 Digital Economy Act 2017, s.18.

III. The most relevant jurisprudence

III.1. Introduction

In the absence of an overarching general statutory right to privacy, the jurisprudence of the UK courts has developed in a manner that seeks to reflect an appropriate balance between Articles 8 (Right to respect for privacy and family life) and 10 (Right to freedom of expression) ECHR, brought into domestic law by the Human Rights Act 1998. The 1998 Act gives a direct remedy against public bodies (such as the police, local authorities, prison authorities, state schools) which violate the Article 8 rights of others. Where it is alleged that a private body (such as a media organisation) has violated another's Article 8 rights, the claimant must first show that he/she has an existing course of action against the private body (such as a previously recognised tort or other remedy such as that found in the laws of confidence, trespass, nuisance) through which the Article 8 interest can be protected. Once this is established, the UK courts will give an interpretation of domestic law that is consistent where possible with Article 8. Given the constraints of space in the present report, the material below concentrates on the major *post* Human Rights Act development in the field of privacy protection (encompassing both digital and non-digital aspects) namely the tort of misuse of personal information. This new tort has largely superceded the action for breach of confidence in domestic law on account of the fact that it does not depend upon an initial confidential relationship unlike the breach of confidence action.[63] Another claimant-friendly feature of the new tort is that unlike the equity-grounded breach of confidence action, the damages remedy in instances of violation is not at the discretion of the court.[64] An already extensive jurisprudence has developed around the misuse of personal information tort which was first recognised in 2004 in the seminal ruling of *Campbell v Mirror Group Newspapers*.[65]

The contours of this important privacy tort have been further elaborated by the High Court in its 2018 decision *Sir Cliff Richard OBE v BBC & Chief Constable of South Yorkshire*.[66] Of particular significance in privacy disputes concerning media organisations is the ability of the claimant to obtain interim relief in the form of an injunction that prevents disclosure of the specified information in advance of the main trial in which the privacy claim is fully tested. When an injunction is granted to prevent interim publication, this preserves more fully the privacy interest of the claimant at the expense of the media freedom to report matters whose newsworthiness may for a variety of reasons have significantly diminished by the time of the main trial. When an injunction is not granted in interim proceedings and media outlets thus at liberty to publish the contested information, the claimant may feel that he/she has little worth protecting by the time the full action comes to court, even if a remedy in damages is still available in the event of a successful claim. The position at interim stage is governed by the application of s.12 of the Human Rights Act. This is discussed in more detail below. The broad direction of the jurisprudence in this field appears to indicate a greater willingness on the part of the courts to protect individual privacy rights at the expense of the Article 10 interests of media organisations' freedom to engage in news reporting. Finally, recent jurisprudence on the statutory remedy for harassment has clarified a number of issues and these developments are addressed towards the end of this section.

---

63 The distinctness of the new tort has been emphasised, see *Judith Vidal-Hall & Others v Google* [2014] EWHC 13.

64 *Mosely v News Group Newspapers* [2008] EWHC 1777.

65 [2004] 2 AC 457.

66 [2018] EWHC 1837 (Ch) and see for comment 'Sir Cliff wins privacy case' (2018) 168 *NLJ* 5.

III.2. Tort of Misuse of Personal Information

This new tort emerged from litigation involving the model Naomi Campbell against *The Mirror* newspaper after it published a series of stories and photos concerning her treatment for drug misuse. At the start of the case she conceded that as far as the publications revealed the facts of her drug misuse and the fact that she was seeking help for it, these were justified as being in the public interest since Ms Campbell had lied previously to the media about not having a drug misuse problem. It was thus entirely legitimate for the media to lay the correct version about her use of drugs before the public. This much conceded, the central question in the litigation focused upon whether and to what extent the media could report the detail of her treatment. By the slenderest of majorities in the House of Lords (3-2) it was found that Campbell had enjoyed a reasonable expectation of privacy in respect of the details of her medical/addiction problems and that the balance of Campbell's Article 8 interest vs the Article 10 interest of the newspaper came down on the side of Campbell's privacy interest.

The majority reasoned that she was entitled to a remedy for misuse of personal information as follow: a claimant can pursue a remedy without the need for a pre-existing confidential relationship when, as here, the publisher knew or ought to have known that the claimant could reasonably expect his/her privacy to be protected. Where this reasonable expectation of privacy is established, the court must then move to a second stage of analysis and balance the claimant's interest in keeping the material confidential against the recipient's interest in publishing it. It is recognised by the majority that two opposing Convention rights are engaged in such cases. Accordingly, the proportionality of interfering with one has to be measured against the proportionality with interfering with the other. This requires the court to look at the comparative importance of the actual rights raised in the case.[67] The nature of Campbell's Article 8 claim concerned the non-disclosure of medical treatment/health information. Failure to preserve the confidentiality of this information might deter others in the future from seeking appropriate medical assistance and treatment. On the Article 10 side of the balance, it was not clear that the speech here was of the importance that rightly attaches to political speech, intellectual or even artistic expression. The *Mirror*'s details of her treatment (and the photos) did not advance any of these bases for upholding freedom of expression. Whilst it could lawfully be revealed that she had misled the public over the fact of her addiction and that she was trying to do something about it (the lie justified correction by the Mirror), the newspaper was not entitled to publish any further information.[68]

The judges in *Campbell* were clear that the law of confidence had evolved to the point where there is no need for a prior relationship of confidence between the party seeking to restrain disclosure of confidential information and the party wishing to disclose it.[69]

In summary, *Campbell* grounds an action for misuse of personal information where the claimant is able to show (i) a reasonable expectation of privacy; AND (ii) the balance between

---

67 *Re S* [2003] 3 WLR 1425.

68 By contrast, the minority judges were of the view that having misled the public, the claimant forfeited any reasonable expectation of pirvacy. Once this was acknowledged, the disclosure of the additional information regarding the details of her treament was of no more significance that revealing in respect of a person of whom it was known had broken a leg, that the leg was now in plaster.

69 A point made by Sedley LJ in *Douglas v Hello* [2001] QB 967 but see later remarks by Lord Hoffman in *Wainwright v Home Office* [2003] UKHL 53 where he cautioned against judicially-created privacy actions, expressing a preference for statutory regulation in this area.

the claimant's privacy interest and the defendant's interest in publishing the information lies on the side of the claimant.

Attention now turns to a consideration of each element in turn as elaborated by the domestic courts. As will be seen below these elaborations are highly fact-specific and therefore the precedent value of each decision may be quite low.

III.2.1. *Campbell* Stage 1 – Is there a reasonable expectation of privacy?

To answer the question of whether Article 8 engaged in the first place *Murray v Express Newspapers* tells us to look at a range of factors including a) identity/attributes of the claimant; b) nature of activity/nature of information; c) place where it is happening; d) absence of consent; e) effect of disclosure on claimant/family; f) purposes behind publishers' acquisition of information

a) *Identity/attributes of claimant* and e) *effect on claimant – Terry v Persons unknown*.[70] Terry tried to get an injunction to prevent publication of fact that he was having an affair with an ex-girlfriend of a former teammate. The High Court refused the injunction. Terry was considered by the court to be a very robust character and there was no real reason (or supporting evidence) to suppose that he was likely to be caused personal distress by the revelations. The real reason for his action, the court concluded, was to protect his commercial interests. The claimant feared loss of some lucrative commercial contracts if the story was published. Had Terry brought evidence of personal distress and emotional trauma that would be likely caused by the revelations, the likelihood of his action succeeding would have been stronger.

If the claimant is a public figure (defined in cases such as *Spelman v Express Newspapers* as someone who plays a role in public life spanning politics, the economy, arts, social sphere or sport (including sport at the highest level or who aim for the highest level) then there is a reduced expectation of privacy – even if the sportsman/woman does not go on to achieve the very highest level.[71]

At the same time, even public figures are entitled to a degree of privacy in specific contexts. The fact that a person is already well-known may make them especially vulnerable to false complaints or allegations where true information of a particularly sensitive nature is allowed to be published in the context of police investigations into serious crimes. This point was made by the High Court in *Sir Cliff Richard OBE v BBC and Chief Constable of South Yorkshire*.[72] The claimant, a famous singer, was being investigated by police officers as part of their investigation into allegations of historic child sexual abuse. A BBC journalist had found out about the South Yorkshire's forthcoming search of a property owned by Sir Cliff Richard and was there (with a film crew) to record the search. The singer was not at the property at the time of the search. The story with filmed images of police officers gaining entry to the property was broadcast on the BBC's national news programmes. Sir Cliff was at no point arrested or charged with any offence arising out of this investigation. In an action for misuse of personal information, he argued that he had a reasonable expectation of privacy such that neither the fact of the police investigation nor the fact of the search of the property ought to have been broadcast by the BBC. In approaching the question, Justice Mann in the High Court drew on the *Leveson Report into the Culture, Practices and Ethics of the Press* in 2012. *Leveson* had recommended that,

---

70 [2010] EWHC 119.

71 [2012] EWHC 355.

72 [2018] EWHC 1837.

> save in exceptional and clearly identified circumstances (for example where there may be an immediate risk to the public) the names or identifying details of those who are arrested or suspected of a crime shouldn't be released to the press or public.[73]

The High Court also attached weight to the remarks of Sir Richard Henriques in his report into the *Metropolitan Police Service's handling of non-recent sexual offence investigations alleged against persons of public prominence* concerning.[74] The author had observed that digital communications assisted the spread of false allegations and rumours.

> Prominent people are more vulnerable to false complaints than others … They are vulnerable to compensation seekers, attention seekers, and those with mental health problems. The internet provides the information and detail to support a false allegation. Entertainers are particularly vulnerable to false allegations, meeting, as they do, literally thousands of attention-seeking fans who provoke a degree of familiarity which may be exaggerated or misconstrued in their recollection many years later. Deceased persons are particularly vulnerable as allegations cannot be answered.

As a matter of general principle, Justice Mann declared that a police suspect has a reasonable expectation in relation to the facts of (i) a police investigation and (ii) a search of his/her property.[75] This privacy protection, it will be noted, is not limited to suspects in cases involving investigations into child sex abuse offences. It is however liable to be defeated when, on the second stage of the *Campbell* analysis, the Article 10 interests in publication are considered to outweigh Article 8 interests in non-disclosure. The ruling of the court on this matter in *Sir Cliff Richard OBE v BBC and Chief Constable of South Yorkshire* is considered below.

Where the nature of the information relates to children and especially where it is conveyed in photographic form, the domestic courts have been particularly protective. In *Murray v Express Newspapers*, the author JK Rowling and her family were out for a walk along a street in Edinburgh on their way to a family meal. A picture of David, her toddler son, was taken by a photographer with a long lens. The Court of Appeal stated that situations which would not engage Article 8 for adults might well do so for children, thereby entitling parents to sue for damages or get an injunction on behalf of the child/children. In reaching this conclusion, the court noted that David's parents had always tried to keep him out of any publicity surrounding his famous mother. There could be a reasonable expectation that the child would not be photographed without the parents' knowledge and consent, especially when the photographer would have already known that the parents objected to the photographing of their child.

b) *Nature of activity/nature of the information* and (c) *place where it is happening*. Where activities are private these are more likely to give rise to a reasonable expectation of privacy. This is likely to be the case where the information relates to sexual matters. In *Jagger v Darling* the model Elizabeth Jagger (eldest daughter of Mick Jagger) was able to prevent publication of photos based on CCTV stills of her and her boyfriend 'engaging in sexual activities' inside the closed

---

[73] Leveson I *Inquiry into the Culture, Practices and Ethics of the Press* (2012) available electronically at https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press at para.2.39.

[74] R Henriques, *Independent Review of the Metropolitan Police Service's handling of recent sexual offence investigations alleged against persons of public prominence* (2016) para.1.39 available electronically at https://factuk.org/wp-content/uploads/2017/04/Report-Independent-Review-of-the-Metropolitan-Police-Services-handling-of-non-recent-sexual-offence-investigations-1-3-1.pdf.

[75] [2018] EWHC 1837 at para.248.

door of a nightclub.[76] The court held that this was clearly a situation where there was a reasonable expectation of privacy. In *Terry* by contrast the revelation of sexual activity did not relate to the details or images of sexual activity but rather merely the fact of sexual activity.

In *Mosely v News Group Newspapers*[77] [2008] EWHC 1777 News of the World published story with the headline – 'FORMULA One motor racing chief Max Mosely is today exposed as a secret sado-masochist sex pervert.' The article continued 'The son of infamous British wartime fascist leader Oswald Mosely is filmed romping with five hookers at a depraved NAZI-STYLE orgy in a torture dungeon. Mosely…barks ORDERS in GERMAN as he lashes girls wearing mock DEATH CAMP uniforms and enjoys being whipped until he BLEEDS.' This was held by Eady J to constitute private information relating to consensual extra-marital sexual conduct and there was misuse of the private information when it was passed on to the newspaper. It followed that Article 8 was engaged, even though some would say he was behaving immorally by paying prostitutes.

A case going the other way is *Trimingham v News Group Newspapers*.[78] The claimant had already been linked by a number of newspapers with a Government Minister with whom she was said to be having an affair. She had been open about her bisexuality and had not attempted to keep details of previous affairs private. Her previous civil partnership with a woman was celebrated as a public event at a public location therefore she could have no reasonable expectation of privacy in relation to these pieces of information. The photographs of her published by the newspaper did not reveal any significant information in respect of which she had a reasonable expectation of privacy.

Not all information about an individual will engage Article 8. In *Campbell* it was said that trivial or mundane information would not be able to ground a privacy claim. Thus in *John v Associated Newspapers* Sir Elton John wanted to prevent the media from publishing photographs that showed him coming out of his car and walking to his house.[79] The photos showed that his baldness was returning after having had a hair transplant a number of years previously. It was held that the information was too trivial and mundane to warrant protection under Article 8.

c) *Place where it is happening* – (and whether in the public domain). In *ETK v News Group Newspapers* office the question of whether a reasonable expectation of privacy existed arose in the context where an affair between a married man and a colleague at work had become common knowledge at the office in question.[80] It was held that Article 8 was engaged and an injunction was granted by the court. Although the affair had become common knowledge at the office in question, this did not mean that it was more fully in the public domain. The claimant was entitled to expect colleagues to keep the information confidential (and thus away from the newspapers). Accordingly, there was a reasonable expectation of privacy.

a) Children c) Place & d) Consent – Weller v Associated Newspapers[81]

Photographs of a well-known singer and his children when out shopping and later relaxing in a café were taken by an unnamed photographer in Santa Monica, Los Angeles, California. His daughter Dylan was aged 16 at the time. The two other children were the twins who were then

---

76 [2005] EWHC 683.

77 [2008] EWHC 1777.

78 [2012] EWHC 1296.

79 [2006] EMLR 1611.

80 [2011] EWCA Civ 439.

81 [2015] EWCA 1176.

aged 10 months. The article was illustrated with seven photographs which showed the faces of Dylan and the twins. The photographer was asked to stop by the family but instead gave an assurance that faces of the three children would be pixelated. The pictures were later published in an unpixellated form in the defendant *The Mail* newspaper. The defendant argued that an 'innocuous' photograph of a child on a street did not give rise to a reasonable expectation of privacy under Article 8. There was nothing inherently private in showing pictures of an identifiable child out shopping. Moreover, the pictures had been taken by an agency in Los Angeles in a public place where the taking of such photos would have been lawful. In its ruling, the Court of Appeal distinguished between the respective positions of the 10 month old twins and the 16 year old. In the case of 10 month old twins, it is the parents who decide how to protect if at all the privacy of the very young. If the celebrity parents of young children brought their children onto the red carpet at a premiere or an awards night, then this might lessen the degree of privacy that these infants would be able to command. Where, as here, the parents' refusal to consent to photography of their offspring was known to publishers, the courts would attach particular weight to that refusal. In respect of the 16 year old, he/she may be able to exercise his autonomy in a similar way to adults. Moreover, where this person's privacy was violated, a significantly more adverse effect upon the individual could be foreseen. All 3 children had a reasonable expectation of privacy. Notwithstanding that the photographs were taken whilst claimants in a public place, this was in essence a private family outing, It was not trivial or mundane information. Critical to the finding of a reasonable expectation of privacy was that parents did not consent to taking of photo and that all 3 claimants were identified by their surname. In the case of the twins, identification in the photos by surname, children should be protected from the risk of embarrassment and bullying as well as potentially more serious threats to their safety. In case of Dylan, although she had done some modelling for a year, there was clear evidence of an adverse effect of publication in her case. She had been caused genuine embarrassment and considered that the photographs were an intrusion into her private family time with her dad. In respect of the fact that the photography was not unlawful in California, the court said that this fact was properly noted but could not be given substantial weight in the overall analysis.

III.2.2. *Campbell* Stage 2 – The balancing of Article 8 & Article 10 interests

If the claimant does have a reasonable expectation of privacy, the courts turn their attention to the question of where the balance should be drawn between the competing Article 8 and 10 interests. The jurisprudence on this matter indicates that a number of factors will be relevant to determining where the balance lies. These include whether the publication makes a contribution to a debate of general interest;[82] how well known is the claimant; the prior conduct of the person concerned; the content, form and consequences of the publication; and the circumstances in which the photographs were taken. Somewhat unsatisfactorily, some of these factors appear to overlap with elements at Stage 1 of the analysis.[83] It is worth bearing this feature in mind when considering the caselaw. Thus in *Weller v Associated Newspapers* it was found that the photographs of the children did not make a contribution to a discussion of public interest.[84] All the claimants were children with no public profile (twins) or a limited profile (Dylan). They were only of interest to the newspaper because they were the children of a famous musician. These photos were intended to satisfy public curiosity. The fact that Weller

[82] *Von Hannover* (No.2) (2012) 55 EHRR 15.

[83] This point was noted by the High Court in *Sir Cliff Richard OBE v BBC & Chief Constable of South Yorkshire* [2018] EWHC 1837 at para.298.

[84] [2015] EWCA Civ 1176.

had spoken to the media about his family before did not deprive his children of all protection. Visual images of the twins faces had not been published in the media in England.

There can be a public interest in correcting a false image created/promoted by the claimant. *Campbell* itself is one such case. In *Ferdinand v MGN* similarly, there was held to be a public interest in correcting a false image promoted by the claimant.[85] Moreover, the article contributed to a debate as to the claimant's fitness to be a role model in the light of his appointment as England football captain. At the time of the litigation, Ferdinand was a well-known professional footballer with a distinguished playing career and the frequent subject of tabloid stories. The case concerned a story in the *Sunday Mirror* concerning his relationship with a woman he had first met the 1990s when they were both teenagers. According to the article they had drifted apart, then resumed contact for a time. The last time they had met was in 2005 but they had been in communication by telephone and text message between 2007 and early 2010. Having found that the publication engaged Ferdinand's Article 8 rights and that he did enjoy a reasonable expectation of privacy in relation to his relationships with other adults, the court considered the balancing exercise**.** It was noted that one aspect of the public interest can be correcting a false image. In an interview given in another newspaper some years earlier the claimant had projected an image of himself as a reformed character. He admitted in this interview to having been a bit of a 'wild man' in the past but claimed that that part of his life was over. In the present litigation, the court found that there was a public interest in demonstrating (if it were to be the case) that the image is false. Also, a further public interest justification for the story lay in the fact that the claimant had been appointed England football captain and that there were some who would see the captain of the team as a role model. If an individual plays sport at the highest level, this is more likely to render the individual a public figure with a reduced expectation of privacy is somewhat reduced. The *Sunday Mirror* article reasonably contributed to a debate as to whether the claimant was suitable for role of England captain. As the trial judge remarked, Ferdinand's 'relatively recent past failings could legitimately be used to called into question his suitability for the role.'[86]

In the different factual circumstances of *Mosely v News Group Newspapers* by contrast, the High Court found that the Article 10 side of the balance lacked sufficiently weighty interests. No substantial breach of the criminal law was revealed by the disclosures whereas the damage to Mosely's Article 8 interests was substantial, even if it was partially self-inflicted. Justice Eady's approach would have been different if he had found as a matter of fact that the sessions had had a Nazi theme. Had he done so the claims to expose the 'sick' practices of this public figure might have looked stronger since Mosely is the son of the former leader of the British fascists Oswald Mosely. The publishers argued that there was a public interest in revealing the assaults which were committed upon Mosely. This was rejected for two main reasons. First, in the case of the offence known as common assault, consent to an assault is defence in English criminal law. Second, in cases of minor criminal conduct, not every single instance of minor criminal conduct would provide a public interest justification for intrusive journalism that disclosed private sexual matters between consenting adults.

Similarly in in *Sir Cliff Richard OBE v BBC and Chief Constable of South Yorkshire*[87] the Article 10 interests in permitting publication were held to be outweighed by the claimant's Article 8 privacy interests. In this case the High Court stressed the 'very serious consequences' in terms of the personal stigma that was experienced by the claimant after having been identified in

---

85 [2011] EWHC2454.

86 *Ibid* at para.98.

87 [2018] EWHC 1837.

the BBC broadcast. Whilst there was a very significant public interest in learning of the state of police investigations into allegations of historic child sexual abuse, it did not extend to identifying persons under investigation. Moreover in the present case the style of the reporting had been unnecessarily dramatic and sensationalist.[88] Damages amounting to £210,000 were awarded against the BBC.[89] The effect of the judgment is likely to deter media organisations and online websites from identifying suspects in police investigations at least until the point in time that such persons are arrested and/or charged with specific offences.

III.2.3. Injunctive Relief under s.12 of HRA

The ready availability of interim prohibitions on publication in misuse of personal information actions is also worth noting.[90]

Recent practice shows that interim injunctions to restrain publication pending the full trial are likely to be granted more readily in a misuse of personal information action than in say defamation actions. An interim injunction is sought once a legal action has been commenced in order to safeguard the claimant's position until the main trial which may be many months ahead. A publisher may obtain material which it is alleged by the claimant was obtained unlawfully. The claimant will usually wish to prevent the publisher using the material so obtained in advance of the main trial date (at which stage full arguments will be made by each side). Accordingly, the claimant will seek an interlocutory injunction to prevent any use of the materials prior to the commencement of the main trial.

In determining interlocutory applications, the court must apply s.12(3) Human Rights Act 1998 in any assessment of the two stage test from *Campbell*.

This states that:

> No such relief (relief affecting the exercise of freedom of expression) is to be granted so as to restrain publication before trial unless the court is satisfied that the applicant is likely to establish that publication should not be allowed.

The meaning of 'likely' was discussed by the House of Lords in *Cream Holdings Ltd v Banerjee and others.*[91]

The case concerned a claimant company which owned a group of nightclubs. Banerjee was an accountant who worked for the claimant. Upon being dismissed from her employment, Banerjee took copies of documents which she alleged showed illegal activity by the claimant. She then passed these documents to the group of newspapers which owns the *Liverpool Echo* and *Daily Post*. The *Echo* later published details about alleged corruption involving Cream Holdings and a local council official. Cream sought an injunction under s.12 of the HRA to prevent further publication of other information supplied by Banerjee. The defendant publishers resisted the injunction on basis that the information whilst confidential ought to be disclosed in the public interest. The lower courts granted the injunction in favour of the

---

88 Justice Mann referred to a 'significant degree of breathless sensationalism' at para.300 that included shots of a helicopter flying over the property.

89 South Yorkshire Police had already admitted liability for disclosing details of its investigation into Sir Cliff Richard and were ordered to pay a separate (and lesser) sum of damages to the singer.

90 *Calcutt I* observed that 'In England and Wales, an interlocutory injunction will more readily be granted in a breach of confidence case than for defamation. In particular, whereas a defendant in a libel action need say no more than he intends to plead justification and an interlocutory injunction will be refused..., be contrast in the case of breach of confidence he will neeed to make a strong case of public interest.' Cm 1102 (1990) HMSO at para.8.10.

91 [2004] 4 All ER 617.

claimants. On appeal to the House of Lords, the injunction was lifted. It was found that the claimant's chances of success at the full trial were not sufficiently likely to justify an order restraining publication. In his opinion, Lord Nicholls of Birkenhead focused on the correct interpretation of the word 'likely' in s.12(3). What was needed he concluded was a flexible standard. The court should not make an interim restraint order unless the claimant's chances of success at the trial are 'sufficiently favourable' to justify an order. In deciding whether an claimant's chances of success were sufficiently favourable, the courts should in general be 'exceedingly slow' to make interim restraint orders where the applicant has not shown the court that he will probably succeed at trial. There may be cases where it is right to depart from this approach and require a lesser degree of likelihood – such as where the potential adverse consequences of disclosure are particularly serious (e.g. grave risk of injury to a person accused of an offence if his whereabouts are revealed).

III.2.3.1 Cases where an application for an interlocutory injunction succeeded

ETK v News Group Newspapers[92] concerned an affair between a married man (K) and a colleague at work (X). Having ruled that Article 8 was engaged and a reasonable expectation of privacy established, notwithstanding the fact that the affair had become common knowledge at the office in question, the Court of Appeal's attention now turned to the proper balance at the interlocutory stage between the competing Article 8 and Article 10 considerations.

On the Article 8 side of the balance K, X and K's wife all wanted to keep knowledge of the affair out of the media. K and his wife had children and the court found that the children's interests were relevant to the decision whether to grant an injunction and that these interests would be best served by preventing publication. There was, by contrast, very little to put on the freedom of expression side of the scales. Publication of the story at the interim stage of proceedings would have added very little to debates of general public interest. Whilst a prurient interest on the part of the reading public might be satisfied in reading an account of the affair, this did not weigh heavily on the Article 10 side of the balance.

PJS & anor v Newsgroup Newspapers[93]

An interim injunction was sought by PJS and his partner to protect the privacy interests of themselves and their children pending a full trial against *Sun on Sunday*. In the full trial, the claimants were seeking a permanent injunction to prevent publication of details of a three way sexual encounter between PJS (described as being in the entertainment business and now married to LMA – described as 'well-known' and also in the entertainment business) and two other adults AB & CD. The latter had approached the *Sun on Sunday* to see if it would be interested in paying for and publishing details of this encounter. When the newspaper's editor approached PJS for comment, PJS went to court to get an injunction in advance of publication. This was granted by the lower courts. A few months later a US magazine published the names and story details in hard copy form. Lawyers for PJS managed to get injunctions in the United States blocking virtually all online versions of the journal appearing outside the US. There followed speculation on social media that in some cases accurately stated the real identities of PJS & LMA. At this time, a google search using the real name of PJS connected him to the threesome story. When it became apparent that social media sites were carrying this information, the *Sun on Sunday* went back to court to have the original injunction lifted on the basis that, as any damage to PJS and LMA had already occurred and the real names of PJS and LMA were now in the public domain, the injunction could no longer be said to serve any useful

92 [2011] EWCA Civ 439.

93 [2016] UKSC 26.

purpose. In fact, lawyers for the newspaper argued, the law was being made to look ridiculous when it was so obviously being flouted. The Court of Appeal agreed and lifted the interim injunction.

On appeal to the UK Supreme Court, the injunction was restored on a majority 4-1 decision by the Supreme Court Justices. On the matter of balancing the respective Article 8 and 10 claims, the majority noted that the value of the type of expression at issue here was at the 'bottom end of the spectrum'. Compared to 'high end' value political expression, this was gossip about the lives of celebrities who performed no public function.[94] So the Article 10 'weight' was not a heavy one at all. There was no 'public interest' here. Public curiosity did not equate to public interest. On the other side of the scales, the Article 8 interests of PJS, LMA and their children would be caused additional damage if tabloid newspapers were able to name in hard copy form PJS and LMA, notwithstanding the existing damage caused by the fact that social media sites accessible here in England had already identified the claimants. It followed that an injunction would protect PJS and LMA from at least some of the distress and damage that would follow from the renewed levels of media interest and intrusion if the interim in junction were lifted. The Supreme Court ordered the injunction to continue in force until the full trial whenit would be reconsidered.[95]

III.2.3.2 Cases where an application for an interlocutory injunction failed

Author of a Blog v Times Newspapers[96]

The claimant blogger (a serving police officer) at the centre of events self-identified as 'Nightjack'. He provided his readers with an insider's account of modern policing, detailing a no holds-barred account of the daily lot of an officer, far removed from the glossy fictional dramas beloved of television producers. Some blogs were openly critical of politicians and, in an indication of the quality of Nightjack's work, the author won the prestigious Orwell prize for online political writing in 2009. *The Times* newspaper had learnt of the blogger's real identity and proposed to reveal this when the claimant sought an injunction to prevent publication of his real identity. The claim came before the High Court.

The claimant needed to show that he/she had a reasonable expectation of privacy under Article 8 of the European Convention in relation to the information that the defendant wished to publish (stage 1) and, assuming the claimant could satisfy stage 1, that there was no countervailing public interest in freedom of expression to override that reasonable expectation of privacy (stage 2). At stage 1, Eady J noted that the cases in which a reasonable expectation of privacy had so far been recognised by the courts had involved information concerning sexual relationships, physical and mental health, financial affairs or domestic and family arrangements. There had not been a case when an anonymous blogger had sought to invoke Article 8 to prevent his/her identity being revealed to the public. In the absence of relevant caselaw, the judge placed considerable weight on an earlier High Court decision in *Mahmood v Galloway and another* where an undercover investigative reporter for a Sunday newspaper had failed to prevent publication on a website of two photographs of himself.[97] One of the

---

94 *Hannover v Germany* (No.1) [2005] 40 EHRR 1.

95 In dissent Lord Toulson doubted that the additional damage caused by the lifting of the injunction really would amount to much since it was now common knowledge who the threesome were and what they got up to. The story was out there and not going away – injunction or not. As for the children there were steps the parents could take to shield them from the immediate publicity. In any case it was inevitable that he children would learn in later life what was being said now.

96 [2009] EWHC 1358.

97 [2006] EMLR 26.

photographs was taken while the reporter was at work for the newspaper and was held not to give rise to any privacy claim. The other was a passport photograph, taken for the purpose of work. This too was deemed to lack the necessary element of privacy inherent in a family photograph intended for home viewing only. It followed that neither image engaged Article 8 for the purposes of stage 1 of the application for an injunction. As the photographs of the undercover reporter lacked the necessary element of private information, so too Justice Eady reasoned did the name of the blogger. In a sound bite that would have sent alarm bells ringing in the blogosphere, Justice Eady concluded that 'blogging is essentially a public rather than a private activity' with the consequence that the blogger could not establish a reasonable expectation of privacy for the purposes of injunctive relief.

Had Justice Eady felt it necessary to examine the stage 2 balance – 'privacy versus countervailing public interest in allowing publication of the blogger's name', he indicated that *The Times* would have succeeded on this point also. The purpose behind the application to prevent *The Times* revealing his identity to the world at large was to protect the blogger from disciplinary measures being taken by his employers (immediate superior officers had been told by *The Times* of the identity of the blog's author) and from causing difficulties in his working relationships with fellow officers. However Eady J held that it was not part of the court's function to prevent more senior police officers *or* the public from learning about this officer's conduct. Indeed, the public's ability to assess the worth of the blogger's contributions to public debate would be enhanced by knowledge of the identity of the blogger.[98]

Hutcheson v News Group Newspapers[99]

Hutcheson, the father-in-law of the celebrity television chef Gordon Ramsay, wanted an injunction to stop publication of the fact that he (Hutcheson) had fathered two children with his mistress. The context for this litigation was that Hutcheson had been involved in a very public dispute with Ramsay after the latter had sacked him. Hutcheson had subsequently attacked Ramsay in the media over the way Ramsay ran his companies and claimed that Ramsay was responsible for the breakdown in relations between Ramsay's wife and her parents. The Court of Appeal refused to grant an injunction. Basing itself on the point made by *Terry* earlier, namely that there should be a degree of freedom to criticise persons in public life, the court noted the background of anti-Gordon Ramsay stories that had been supplied to the media. Against this context, the story about Hutcheson's second family could be said to show Ramsay's account of events leading to the breakdown in family relations.

McClaren v News Group Newspapers[100]

An injunction was also refused in a case involving the former England football manager Steve McClaren whom the court considered to be a public figure on the basis of the earlier decision in *Spelman*. McClaren had not tried to prevent a previous story about an extra marital relationship being published but had decided instead to put his own account of his private life into the public domain, telling readers that he was happily married and his marriage would survive. *The Sun* newspaper now wanted to publish an account of the 'kiss and tell' variety where another woman wished to reveal details of her sexual encounter with Steve McClaren. The High Court refused to grant an injunction preventing publication of the story. It was true that the information was of such a character (sexual, private life) as to attract a reasonable expectation of privacy. However, when considering the balance between the Article 8 and 10

98 For commentary see I Cram, *Citizen Journalists* (2016, Edward Elgar, Gloucester) at pp.95-99.

99 [2011] EWCA Civ 808.

100 [2012] EWHC 2466.

interests raised by the particular facts of the case, this fell on the side of allowing publication at the interim stage. McClaren was a public figure and, like the England football captain Ferdinand, was someone from whom the public could expect a higher degree of personal conduct.

III.3. Protection from Harassment Act 1997

III.3.1. Generally applicable jurisprudence

Judicial guidance on liability for harassment under the 1997 Act has clarified a number of issues arising under the legislation. The conduct in question has to be aimed at an individual (not necessarily at the claimant)[101] and calculated when viewed objectively to cause alarm or distress to that individual.[102] Conduct which falls short of harassment (and therefore outsider the Act) might include unattractive, even unreasonable behaviour.[103] Instead, the conduct targeted by the Act is of a different, considerably more serious order one that an objective person would consider oppressive and unreasonable.[104] It occurs typically where one person engages in intensely personal conduct towards another which

> may range from using actual physical force (against that person) … or more subtle but nonetheless intimidating conduct. In each case the defendant will (or should be) aware of the effect which his conduct is having on the claimant.[105]

Context is of course hugely relevant to determining whether conduct has stepped over from unreasonable behaviour into that which is oppressive and unreasonable. What might be classed as harassment in a business or public service environment might not so classed on the factory floor or on the football terraces.[106] Liability under the 1997 Act can be incurred by corporate bodies. Thus in *Ferguson v British Gas Trading Ltd* repeated demands for payment and threats of legal action generated by the defendant's computer billing system was considered capable of constituting harassment.[107] In *Roberts v Bank of Scotland* a customer whose account was excessively overdrawn received 507 telephone calls from the Bank over a thirteen month period. Though in breach of her contract with the bank, the Court of Appeal held that the bank had nonetheless bombarded the claimant with endless phone calls and that this constituted harassment under the 1997 Act causing her distress. She was awarded £7,500 in compensation.[108]

Guidance from the case law on the nature of the defences indicates that what counts as reasonable conduct under s.1(3) of the 1997 Act depends on the circumstances of the case.[109]

---

[101] *Levi v Bates* [2015] EWCA Civ 206. This means that the partner of a person who is being stalked is able to take an action against the stalker, despite not being the target of the stalker.

[102] *Dowson v Chief Constable of Northumbria Police* [2010] EWHC 2612 (QB).

[103] *Majrowski v Guy's and StThomas's NHS Trust* [2005] EWCA Civ 251 at para 30.

[104] *Green v DB Group Services* [2006] EWHC 1898 (QB); *Thomas v News Group Newspapers Ltd* [2001] EWCA Civ 1233.

[105] *Jones v Ruth* [2011] EWCA Civ 804 at para.24.

[106] *Conn v Sunderland City Council* [2007] EWCA Civ 1492. There Gage LJ noted that conduct that 'might not be harassment on the factory floor or in the barrack room might well be harassment in the hospital ward and vice versa' at para 12.

[107] [2009] EWCA Civ 46.

[108] [2013] EWCA Civ 882.

[109] *R v C* [2001] EWCA Crim 1251.

III.3.2. Specific harassment issues arising via print and digital media

A number of useful dicta have emerged from litigation in the courts regarding when 'speech' can amount to harassment under the 1997 Act.[110] In *Thomas v News Group Newspapers* it was held that a newspaper could in theory be guilty of harassment in respect of a series of articles.[111] On the facts in *Thomas* a series of newspaper articles were published in which it was alleged that, had it not been for the fact that Thomas was black, then two police officers would not have been taken to a disciplinary hearing over remarks made about a third party in Thomas' presence. The Court of Appeal found that the articles repeatedly and unnecessarily referred to Thomas as a 'black clerk' and it was forseeable in the circumstances that the articles would be likely to provoke a racist reaction and that Thomas would have been caused distress. There are obvious Article 10 ECHR issues here however which the Court of Appeal was alive to. The 1997 Act must be read where possible in a way which strikes an appropriate balance between the Article 8 rights of the claimant and the Article 10 rights of media organisations (as speakers) and the public (as audience). Put another way, the 1997 Act must not be read in a way that impermissibly encroaches upon Article 10 freedoms. Restrictions upon expression that flow from the 1997 Act must thus be proportionate and for a legitimate purpose.[112] Lord Phillips MR noted that generally speaking media criticism of an individual published in a series of articles, even if expressed in robust language, would not constitute unreasonable conduct. It seems to have been accepted however that the publication of a series of articles which were calculated to incite racial hatred of an individual (or hatred on religious or sexual orientation grounds) could constitute harassment of that individual where it was foreseeable that the resulting publicity would cause the individual distress and alarm. This would be considered an abuse of media freedom and as such actionable. Some commentators take the view that the dissemination on more than one occasion by a media outlet of the address or email/Twitter account details of a celebrity and encouragements to readers to contact that person might be considered harassment under the Act.[113] Separately, there is the issue of whether letters (in the printed press) and posts and comments by readers of an online media publication made in response to an article published in the online version of the newspaper/magazine could constitute harassment. Does the fact that the publishers of an online newspaper/magazine expressly disassociate themselves from posts subsequently made by members of the public enable publishers to resist a harassment claim brought by a claimant who alleges that the original article prompted the subsequent posts? The point has still to be settled in English Law.

Campaigns that target an individual by making a series of (i) defamatory and/or (ii) factual disclosures may be made subject to injunctions issued under the 1997 Act. These instances of 'vilification' might entail obsessive emailing to the victim,[114] website publication of false allegations of wrongdoing,[115] and inviting others to supply details of a third party's whereabouts, having published allegations of wrongdoing by that party.[116]

---

[110] Speech is expressly mentioned in s.7(4) as falling within the definition of 'conduct' prohibited by s.1.

[111] [2001] EWCA Civ 1233.

[112] *Trimingham v Associated Newspapers Ltd* [2012] EWHC 1296. Clearly the protection of the 'rights of others' in Article 10(2) would include the right to respect for private life in Article 8.

[113] Tugendhat & Christie *The Law of Privacy and the Media* (3rd edn) (2016, OUP, Oxford) at 284-5.

[114] See *R v Debnath* [2005] EWCA Crim 3472 where a permanent injunction was issued to prevent the defendant from publishing any information about her victim and his fiancée.

[115] *Law Society v Kordowski* [2011] EWHC 3185 concerning publication of false allegations on a website *Solictors from Hell*.

[116] *Levi v Bates* [2015] EWCA Civ 206.

IV. The Nature of the Right

IV.1. European legal framework

UK laws seek to comply with the requirements of both the European Convention on Human Rights (Articles 8 & 10) and, until its departure from the European Union, the EU Charter on Fundamental Rights Articles 7 & 8. The latter is binding on the UK. Domestic laws that inconsistent with the EU Charter may be disapplied to the extent that they are inconsistent with the Charter.[117] In respect of European Convention on Human Rights, public bodies (including the courts) are expected to conduct themselves in accordance with relevant Convention Articles by virtue of the Human Rights Act 1998 unless a domestic Act of Parliament requires them to act differently.[118]

ECHR

Article 8 Right to Respect for Private and Family Life

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.

Article 10 Freedom of Expression

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

EU Charter of Fundamental Rights

Article 7 of the Charter on Fundamental Rights provides that:

> Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 states in respect of personal data that:

---

[117] *Bekharbouche and another v Embassy of the Republic of Sudan* [2015] EWCA Civ 33.

[118] S.6, HRA 1998.

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

GDPR (General Data Protection Regulation)

Article 17

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

   (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

IV.2.Data Protection Act 2018

As noted in the *Introduction* above, in July 2018 *Facebook* was found by the Information Commissioner to have violated principles relating to the security of users' data and failing to be explicit about how users' data would be accessed by others. The violations occurred in 2014-15 when the social media platform allowed an app to harvest data from the profiles of approximately 87 million *Facebook* users that was then used by *Cambridge Analytica*. *Facebook* was fined the maximum sum permitted under the 1998 legislation then in force. The data thus obtained was used by *Cambridge Analytica* and others[119] to target voters in the UK referendum on continued EU membership. In August 2018 another company *Lifecycle Marketing (Mother and Baby) Ltd* (otherwise known as *Emma's Diary*) was fined £140,000 (again under the old 1998 Act's provisions) for failing to disclose to its one million+ users that personal information provided by them would be sold to marketing companies to create profiles of new mothers and then used by political parties in the 2017 General Election campaign to target individual voters.[120]

Events surrounding data protection violations by *Facebook* and *Emma's Diary* have pointed up the increased frequency of micro-targeting or nudging of voters in elections and referenda through the use of personal data. Whilst we may have become accustomed by now to personalised advertisements on social media, the practices revealed in 2018 raise issues that go to the core of the democratic politics and the means by which parties communicate with voters. It is true that targeting of specific voters (and specific constituencies) has long been a feature of pre-digital era campaigning in local and regional elections. However, digital

[119] The Information Commissioner has said that companies with links to *Cambridge Analytica* 'may still retain' data about UK voters, A Hern & D Pegg, 'Facebook fined for data breaches in Cambridge Analytica scandal' (2018) *The Guardian* July 11.

[120] See the press release from the Information Commissioner's Office on August 9, 2018 at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/. The Labour Party was able as a result to send targeted direct mail to new mothers in marginal seats about its policies for families.

technology allows marketing companies and political parties that employ them to acquire very precise details about an individual. It is not always apparent that individuals have given their full and informed consent to the acquisition and use of extensive personal data by third parties.

Under Article 17 of the GDPR, a data subject has the right to secure the erasure of personal data held by data controllers including search engines and digital intermediaries such as providers of internet access and browser services.[121] This right is acquired where the processing of the data is no longer considered necessary for the exercise of freedom of expression and information. Though clearly broader than the 'right to be forgotten' established by the CJEU in *Google Spain*, Article 17 GDPR will likely be used in domestic law to remove personal data from search engines and browsers with the consequence that public access to information, especially historic records of individuals' previous conduct such as their previous convictions will be made more difficult. An indication of how matters may develop domestically was provided by the High Court in April 2018 in *NT1 & NT2 v Google*.[122] This is the first case in English law to rule on the matter. Two businessmen sought to have links to articles about their separate criminal convictions removed. The convictions dated from over ten years previously and each was 'spent' for the purposes of the Rehabilitation of Offenders Act 1974. The first claimant had been sent to prison for four years for his role in a criminal conspiracy that affected members of the public. The second claimant had pleaded guilty to criminal conspiracy charges in respect of a 'controversial' business that had provoked public opposition and criticism on environmental grounds. He was sentenced to a short period of custodial remand. Both cases were reported in the media at the time. These published reports could be retrieved via a Google search. Each man now submitted a de-listing request to Google which was declined. In balancing the competing interests at stake in each claim, Warby J. held that Google must action NT2's de-listing request whilst being entitled to refuse NT 1's request. The basis of this distinction was as follows: NT1 still plays a limited role in public life. The information in question was not shown to be inaccurate and relates to his business life, not his personal life. He had not accepted his own culpability for the conduct which led him to be convicted and continued to show no remorse whilst remaining in business. In the light of these factors the ongoing availability of his past conviction 'serves the purpose of minimising the risk that he will continue to mislead as he has done in the past.'[123]

In respect of NT2, whilst he was also still a public figure, albeit a less prominent one now than at the time of his conviction, there was clear evidence that the availability of the data has had a strongly adverse effect on his family life and in particular his school age children. He has also found it hard to obtain personal financial services such as bank accounts as a result of the ongoing publicity. He has acknowledged his past wrongdoing and expressed genuine remorse. He is unlikely to repeat his crimes. His new business activities do not lie in the area to which the previous convictions relate. Accordingly, the past offending was deemed of little relevance to anyone's assessment of his current/future business activities. Google were ordered to de-list NT2 meaning that henceforth no link could be traced via Google that connected NT2 to his previous conviction.

In general terms, there must be a concern that search engines and other digital intermediaries might respond to ill-founded 'right to be forgotten' requests by removing content that is not unlawful. The financial penalties for non-removal provide a strong motive to err on the side of excessive as opposed to insufficient censoring of content. The provider of the disputed content

[121] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311.

[122] [2018] EWHC 799.

[123] *Ibid*. at para.170.

is normally never afforded an opportunity to defend the content nor to be given an explanation of the basis for the request. This can potentially undermine important democratic interests in informed discussion on matters of public interest. It is likely that powerful individuals and companies whose affairs and past conduct might well merit public scrutiny will use Article 17 GDPR and the 'right to be forgotten' to make it considerably harder to access adverse comment and information whilst putting out their own possibly untrue, or disputed version of events. As Keller puts it, 'It is already too easy for individuals or companies to raise dubious legal claims against content they disagree with, and pressure private Internet platforms to take it down…If we want to protect culture, commentary and creativity online, private Internet companies need the confidence to resist the right to be forgotten requests that have no basis in European law.' [124]

IV.3. Restrictions on privacy interests – National security & prevention/detection of crime

State interests in national security and the effective investigation and detection of crime obviously require at certain times interference with natural and legal persons' privacy interests The Snowden revelations in 2013 pointed however to the unauthorised interception and sharing among US & UK national security agencies of private digital communications across the world through programmes such as *Tempora*. GCHQ boasted in 2011 of having

> 'massive access to international communications … we receive upwards of 50 *Billion* events *per day* (…and growing)'[125]

In a democratic state under the rule of law, it is of paramount importance that executive agencies act under clearly established and precisely stated legal powers consented to in advance by the elected representatives of the people.

The Investigatory Powers Act 2016 represents yet another attempt by the UK Parliament (after RIPA 2000 & DRIPA 2014) to construct an effective legislative scheme to regulate this complex and hugely controversial area. It is considered by some to have missed an opportunity to simplify what was an already complex area. One leading commentator has described the Act as 'opaque' and 'unnecessarily unwieldy'.[126]

There are two principal concerns in relation to state surveillance upon the contents and meta data of personal communications. First is that inevitably UK laws and parliamentary oversight of security agencies' practice have lagged behind the data interception programmes of security agencies. Thus the legal framework will always lag behind technological developments and require regular review and revision if it is to be fit for purpose.

The second main concern as evidenced by courts analysis in cases such as *Secretary of State for Home Dept v Davis, Watson and others*[127] and *R (on the application of Liberty) v Home Secretary and Foreign Secretary*[128] is that recent legislative reforms have not managed to properly respect ECHR and EU Charter privacy protections for citizens. National laws have thus been found to

---

[124] D Keller, 'The new, worse 'right to be forgotten'' https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/.

[125] Cited in G Greenwald, *No Place to Hide Edward Snowden, the NSA and the Surveillance State* (2015, Penguin Books, London) at p.100.

[126] S McKay *The Investigatory Powers Act* 2016 (Blackstone's Guide) at 24.

[127] [2018] EWCA Civ 700.

[128] [2018] EWHC 975 (Admin).

lack transparency and/or interfere disproportionately with citizens' private data records. In one instance, domestic legislation granted powers of interception to bodies wholly unconnected with the protection of national security or the prevention and detection of crime in violation of the EU Charter on fundamental rights.[129].

As the CJEU had previously found in *Digital Rights Ireland* 'bulk' data gathering warrants are especially problematic in ECHR proportionality terms because of the sheer volume of individuals whose private lives are put under surveillance.[130] The vast majority of such persons will not have been suspected of involvement in terrorist/criminal activities prior to being put under surveillance. This part of the Act was passed after the Investigatory Powers Tribunal (which examined complaints under the previous RIPA 2000 and the Telecommunications Act 1984) ruled in October 2016 that MI5, MI6 and GCHQ Cheltenham had been unlawfully amassing huge volumes of personal data under these earlier laws.[131] The gathering had taken place in secret over many years without being publicly acknowledged in Parliament until 2015.

In separate revelations to emerge in the course of legal proceedings brought by Libyan dissidents against the UK Government alleging state involvement in their rendition to Libya, it emerged that security service agencies had since 2010 secretly authorised their staff to intercept certain classes of lawyer-client communications.[132] The Government conceded that these authorisations had been in breach of Article 8 of ECHR in February 2014 specifically on the ground that the safeguards contained within the guiding authorisations had not been made sufficiently public. It stated that the agencies would now work with the Interceptions Commissioner to make sure that future interceptions were compliant with Convention rules. A new Code of Practice setting out *inter alia* the terms of security services' interception of such communications was published in 2016.[133]

IV.4. The emerging tort of misuse of personal information & protection from online forms of harassment – developments at common law

As a relatively recent judicial innovation, the tort of misuse of personal information offers an important means of preserving individual privacy interests where threatened by either traditional and digital journalism. The implications of *Sir Cliff Richard OBE v BBC and Chief Constable of South Yorkshire* where the tort of misuse was applied in novel circumstances may yield further and significant extensions of privacy protection in future litigation. The High Court's clear distaste for what it deemed to be 'sensationalist' reporting informs a judgment that may be considered to undermine the ideal of open justice and the informed oversight via media reporting of policing in individual cases where a clear and compelling public interest exists. As such, it could perversely jeopardise confidence in the police especially in relation to

[129] *R (on the application of Liberty) v Home Secretary and Foreign Secretary* [2018] EWHC 975 (Admin).

[130] Joined Cases C-293/12 and C-594/12 and see further D Anderson QC in *A Question of Trust* (2015) https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf at para 5.31.

[131] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others* [2016] UKIPTrib 15_110-CH.

[132] A Travis & O Bowcott, 'UK admits unlawfully monitoring legally privileged communications' *The Guardian* (2015) February 18.

[133] https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2016 see pp.16-21.

prominent individuals.[134] In circumstances where suspects enjoy a general right to anonymity, it is all too easy to imagine unfortunate scenarios in which misinformation and rumour about others wholly unconnected with the police investigation begin to circulate. More importantly still, it might be considered unhelpful that the ruling obstructs the coming forward of others (as witnesses and victims) who may have valuable information about a named suspect that they wish to provide police investigators. The damaging impact upon the successful prosecution of offenders is plainly an unwanted consequence of the ruling. The beneficiaries of this ruling include not only those innocent of any crime (such as the claimant) but also (temporarily at least) those who will be found in due course to have broken the law. The effect of the judgment is likely to deter media organisations and online websites from identifying suspects in police investigations until the point in time that such persons are arrested and/or charged with specific offences.

Finally, the adaption by the courts of the Protection from Harassment Act 1997 to the digital age would appear to offer some measure of privacy protection to an individual in circumstances where say details of an email address/ Twitter/Facebook account or mobile phone number are supplied to the public. Where these details were supplied separately in both hard copy form and online, it may be that a 'course of conduct' by the disseminator can be established. By way of comment, it may be thought that this extension of the 1997 Act regulates conduct that would not have been in the contemplation of legislators at the time of the Act's passage into law. Whether such judicial creativity oversteps the constitutional bounds of the judicial function in a democracy is of course a moot point.

[134] See thus R Greenslade, 'Why Cliff Richard's case against the BBC should worry us all' (2018) *The Guardian* April 17 at https://www.theguardian.com/commentisfree/2018/apr/17/cliff-richard-bbc-court-case-police-press-media.

V. Conclusions

Several contradictory currents can be detected concerning legal developments in digital privacy. At the outset, it is a given that technology will continue offer governments and corporations who invest in it for diverse reasons novel means of accessing others' data. The business model of the corporations that own search engines and social media platforms depends upon those platforms ability to extract data from users and sell the same on to suppliers of goods and services wishing to be connected to new customers. Allowing users to more readily alter and enhance their privacy settings may offer one strategy for boosting individuals' data protection. There will however always be an economic imperative to facilitate the growth of markets via targeted marketing that lies in tension with ideas of user privacy. The *Cambridge Analytica* story further indicates that, without adequate and enforceable data security rules social media platforms may be vulnerable to data mining on a massive scale. Whether GDPR and the Data Protection Act 2018 are up to the task of tackling the improper accessing and selling on of personal data remains to be seen. It is still not clear what role *Facebook* may have played in these practices as actions for damages by disgruntled *Facebook* users look set to come before the courts.[135] However and for the time being, the cast majority of these actions will be determined under provisions laid down in the previous and less user-friendly Data Protection Act 1998 since the allegations are confined to a period when the 2018 Act was not in force. It may therefore be sometime before an assessment can be made regarding the fitness for purpose of GDPR and the UK's 2018 Data Protection Act. Separately, the judges' understanding of the 'right to be forgotten' and its relationship to Article 17 of GDPR will become clearer in specific factual settings as individual disputes between individuals and search engines/internet browsers/ journalists reach the doors of the court. There is a legitimate anxiety here that the shift towards enhanced privacy protection may be achieved on occasions at the expense informed scrutiny of public figures and material whose publication has a strong public interest justification. At the same time, it is also worth recalling that the law will always lag behind technological developments and thus be forced in to a responsive regulatory mode to protect individual privacy. It seems clear that the technological advances of today and tomorrow may be put to uses that straddle legal 'grey' areas where the application of previously crafted laws and regulations is unclear. This suggests that the task of law-making bodies entrusted with reviewing and maintaining appropriate levels of data privacy in law will be on-going.

Another significant ongoing challenge to the privacy interests of digital users is that posed by the demands of national security (counter terrorism) and crime detection/prevention. It is now conceded that UK security agencies were engaged for some time after 9/11 in the unlawful interception of communications data and content. At the time of the revelations of Edward Snowden, the UK possessed more CCTV cameras than anywhere else.[136] Thanks to Snowden, we now know GCHQ operated its *Tempora* programme to access the servers of *Google* and *Facebook* much as the US National Security Agency obtained access under its *Prism* programme. GCHQ and NSA collaborated over *Upstream* to enable access and interception of cable and network communications. The data is loaded into *XKeyscore* which enables the instant extraction of subsets of data. As Lanchester remarks, considerable public monies have also been invested in incentivising IT companies to create secret security weaknesses into

[135] 'UK Group threatens to sue facebook over Cambridge Analytica' (2018) July 31 see https://www.wired.com/story/uk-group-threatens-to-sue-facebook-over-cambridge-analytica/.

[136] J Lanchester, 'The Snowden files: why the British public should be worried abut GCHQ' (2013) *The Guardian* October 3 citing an estimate made by Cheshire Police in 2011.

supposedly secure, commercially available products. In the UK for example it is known that GCHQ working with the NSA has for almost a decade been able to switch Apple *I*phones *I*pads on and off without users' knowledge and acquire information about users' lives.[137]For those concerned that the state's gathering of intelligence data adheres to overarching democratic ideals such as the rule of law and the informed consent of citizens and their elected representatives in whose names and by whose authority the security agencies act, two features of recent state practice stand out; namely (i) the lack of judicial prior authorisation of particular aspects of data surveillance under the Investigatory Powers Act 2016; and (ii) the use of surveillance powers for purposes entirely unrelated to those set out by the 2016 Act. Recall in this regard the High Court ruling in April 2018 in *R (on the application of Liberty) v Home Secretary and Foreign Secretary*[138] that state bodies including local authorities and financial regulators were granted unlawful access under Part IV the 2016 Act to the communications data records of telecommunications companies without the need to show a purpose connected to the investigation of serious crime or terrorism. The dangers of state overreach must *post* Snowden be firmly and constantly at the forefront of legislators' minds. In the meantime, we await to see what amendments the UK Government proposes in respect of Part IV of 2016 Act to better safeguard the legitimate privacy concerns of users.

Turning finally to judicial development of privacy protection at common law, the tort of misuse of personal information offers considerable scope to preserve individual privacy interest in the face of intrusive forms of both traditional and digital journalism. It is possible however to have some reservations about the direction of judge-developed law in the aftermath of *Sir Cliff Richard OBE v BBC and Chief Constable of South Yorkshire* where the tort of misuse was applied in novel circumstances.[139] The BBC announced in August 2018 that it would not be appealing the judgment in the case.[140] The reasoning of Justice Mann might be thought by some to pose a risk to the informed oversight via media reporting of policing in individual cases where a clear and compelling public interest in disclosure exists.

[137] Der Spiegel at http://www.spiegel.de/media/media-35662.pdf.

[138] [2018] EWHC 975 (Admin).

[139] [2018] EWHC 1837 (Ch).

[140] 'Sir Cliff Richard privacy case: BBC will not go to Court of Appeal' (2018) August 15 https://www.bbc.co.uk/news/uk-45183421.

List of legislative acts quoted

Computer Misuse Act 1990

Contempt of Court Act 1981

Criminal Justice Act 1988

Criminal Justice and Courts Act 2015

Criminal Justice and Immigration Act 2008

Criminal Justice and Police Act 2001

Data Protection Act 1998

Data Protection Act 2018

Data Retention and Investigatory Powers Act

Digital Economy Act 2017

Human Rights Act 1998

Investigatory Powers Act 2016

Police and Criminal Evidence Act 1984

Protection from Harassment Act 1997

Protection of Children Act 1978

Regulation of Investigatory Powers Act 2000

Rehabilitation of Offenders Act 1974

Serious Crime Act 2015

Sexual Offences Act 2003

List of cases

Domestic Court/Tribunal judgments

AG v Leveller [1979] AC 440

Author of a Blog v Times Newspapers [2009] EWHC 1358

Bekharbouche and another v Embassy of the Republic of Sudan [2015] EWCA Civ 33.

Campbell v MGN [2004] 2 AC 457

Conn v Sunderland City Council [2007] EWCA Civ 1492

Cream Holdings Ltd v Banerjee and others [2004] 4 All ER 617

Douglas v Hello [2001] QB 967

Dowson v Chief Constable of Northumbria Police [2010] EWHC 2612

ETK v News Group Newspapers [2011] EWCA Civ 439

Ferdinand v MGN [2011] EWHC 2454

Ferguson v British Gas Trading Ltd [2009] EWCA Civ 46

Green v DB Group Services [2006] EWHC 1898

Hutcheson v News Group Newspapers [2011] EWCA Civ 808

Jagger v Darling [2005] EWHC 683

John v Associated Newspapers [[2006] EMLR 1611

Jones v Ruth [2011] EWCA Civ 804

Judith Vidal-Hall & Others v Google [2014] EWHC 13

Law Society v Kordowski [2011] EWHC 3185

Levi v Bates [2015] EWCA Civ 206

Mahmood v Galloway & Another [2006] EMLR 26

Majrowski v Guy's and St Thomas's NHS Trust [2005] EWCA Civ 251

McClaren v News Group Newspapers [2012] EWHC 2466

Mosely v News Group Newspapers [2008] EWHC 1777

Murray v Express Newspapers [2008] EWCA Civ 446

NT1 & NT2 v Google [2018] EWHC 799

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others [2016] UKIPTrib 15_110-CH.

PJS & anor v Newsgroup Newspapers [2016] UKSC 26

R v C [2001] EWCA Crim 1251

R v Debnath [2005] EWCA Crim 3472

R (on the application of Liberty) v Home Secretary and Foreign Secretary [2018] EWHC 975 (Admin).

Re S [2003] 3 WLR 1425

Roberts v Bank of Scotland [2013] EWCA Civ 882

Secretary of State for Home Dept v Davis, Watson and others [2018] EWCA Civ 700

Sir Cliff Richard OBE v BBC & Chief Constable of South Yorkshire [2018] EWHC 1837 (Ch)

Spelman v Express Newspapers [2012] EWHC 355

Terry v Persons Unknown [2010] EWHC 119

Thomas v News Group Newspapers Ltd [2001] EWCA Civ 1233

Trimingham v Associated Newspapers Ltd [2012] EWHC 1296

Wainwright v Home Office [2003] UKHL 53

Weller v Associated Newspapers [2015] EWCA Civ 1176

CJEU cases

Digital Rights Ireland (2014) C-293/12 & C-594/12

Google Spain Sl v Agencia Espanola de Proteccion de Datos & Gonzalez (2014) C-131/12

European Court of Human Rights cases

Hannover v Germany (No.1) [2005] 40 EHRR 1

Hannover v Germany (No.2) [2012] 55 EHRR 15

Marper v UK [2009] 48 EHRR 50

Select Bibliography

Books

D Cole, F Fabbrini & S Schulhofer, *Surveillance, Privacy and Trans-Atlantic Relations* (2018, Hart, Oxford)

I Cram, *Citizen Journalists: Newer Media Republican Moments and the Constitution* (2016, Edward Elgar, Gloucester)

E Epstein, *How America Lost its Secrets*: Edward Snowden, The Man and the Theft (2017, Knopf Publishing Group, New York)

G Greenwald, *No Place to Hide Edward Snowden, the NSA and the Surveillance State* (2015, Penguin Books, London)

S McKay, *The Investigatory Powers Act 2016* Blackstone's Guide (2017, OUP, Oxford)

H Fenwick & G Phillipson, *Media Freedom under the Human Rights Act* (2006, OUP, Oxford)

J Rowbottom, *Media Law* (2018, Hart, Oxford). Ch.2

M Tugendhat & I Christie *The Law of Privacy and the Media* (3rd edn) (2016, OUP, Oxford)

Articles & Chapters

S Bhaimia 'The General Data Protection Regulation: the next generation of EU data protection' (2018) 18 *LIM* 21

A Cappuccio, 'The private nature of information: a light keeping the courts from straying into the "privacy" penumbra' (2014) 2 *IPQ* 159

Editorial 'Sir Cliff wins privacy case' (2018) 168 *NLJ* 5

D Erdos, 'Data protection confronts freedom of expression on the "new media" internet: the stance of European regulatory authorities' (2015) 40 *ELRev* 531

R Greenslade, 'Why Cliff Richard's case against the BBC should worry us all' (2018) *The Guardian* April 17 at https://www.theguardian.com/commentisfree/2018/apr/17/cliff-richard-bbc-court-case-police-press-media

A Scott, 'An unwholesome layer cake: intermediary liability in English defamation and data protection law' in (eds. D Mangan & L Gillies) *The Legal Challenges of Social Media* (2017, Edward Elgar, Cheltenham)

P Smith '*NT v Google* and the long memory of the internet' (2018) 24 *CTLR* 144

P Wragg, 'A freedom to criticise? Evaluating the public interest in celebrity gossip after *Mosely* and *Terry*' (2010) 2 Journal of Media Law & Practice 295

P Wragg, 'Open Justice and Privacy' (217) *Comms Law* 89

Reports

Calcutt Report of the Committee on Privacy and Related Matters Cm 1102 (1990)

D Anderson QC *A Question of Trust* (2015) at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

J Dawson, House of Commons Briefing Paper *Investigatory Powers Bill* Number 7518, 11 March 2016

R Henriques, *Independent Review of the Metropolitan Police Service's handling of recent sexual offence investigations alleged against persons of public prominence* (2016) available electronically at https://factuk.org/wp-content/uploads/2017/04/Report-Independent-Review-of-the-Metropolitan-Police-Services-handling-of-non-recent-sexual-offence-investigations-1-3-1.pdf

Leveson I *Inquiry into the Culture, Practices and Ethics of the Press* (2012) available electronically at https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press

This study forms part of a wider-ranging project which seeks to lay the groundwork for comparisons between legal frameworks governing the right to respect for private life in different legal systems, and between the ways in which the systems address the challenges that the 'digital age' poses to the exercise of that right.

It analyses, with reference to the United Kingdom, the legislation in force, the most relevant case law and the nature of the right to respect for private life. Chapter 2 describes the concept of a right to respect for private life as it is recognised in UK legislation. This section of materials is subdivided into two parts. The first part outlines statutory protection for privacy interests, including the recently enacted Data Protection Act 2018 that gives domestic effect to the General Data Protection Regulations. The rest of chapter 2 discusses the most prominent set of statutory restrictions or qualifications upon the right. Privacy interests are thus revealed to be limited in the interests of national security and the prevention, investigation and detection of crime including crimes connected to the sexual abuse of children and young persons. Particular sets of laws authorise interception, examination and retention of digital online communications. Relevant obligations imposed on ISPs and telecommunications companies are described as are safeguards against unlawful forms of intrusion into these communications. Chapter 3 provides an overview of relevant jurisprudence in privacy related matters. A central focus of this chapter is the relatively recently developed tort of misuse of personal information. An evaluation of the overall state of UK law is offered in chapter 4. Finally, the conclusion identifies some privacy-related issues that are likely to arise in the near future.

QA-06-18-196-EN-N

This is a publication of the Comparative Law Library Unit
EPRS | European Parliamentary Research Service

Print ISBN 978-92-846-4014-0 | doi:10.2861/53261 | QA-01-16-770-EN-N
PDF ISBN 978-92-846-4016-4 | doi:10.2861/45028 | QA-01-16-770-EN-C