Cambridge Law Journal, **73(2)**, July 2014, pp. 350–377
doi:10.1017/S0008197314000427

BEYOND INFORMATION: PHYSICAL PRIVACY IN ENGLISH LAW

N. A. MOREHAM*

ABSTRACT. *Although English privacy law has developed significantly over the past two decades, it continues to focus almost exclusively on the disclosure of private or confidential information. This article argues that if privacy is to be comprehensively protected, then the importance of physical privacy – which is breached when a person is looked at, listened to or recorded against his or her wishes – must also be recognised. After discussing what physical privacy is and why existing protections for it are inadequate, the author contends that a physical privacy action can, and should, be developed from within English common law.*

KEYWORDS: *Privacy, physical privacy, intrusion, misuse of private information, breach of confidence, intentional infliction of emotional distress, Data Protection Act 1998, Article 8 European Convention on Human Rights, Human Rights Act 1998, surveillance.*

I. INTRODUCTION

A superficial look at the English law of privacy would suggest that privacy is all about the unwanted dissemination of private information. The Data Protection Act 1998 and actions for breach of confidence and misuse of private information focus on confidential information and high profile successful cases invariably involve the (actual or proposed) dissemination of personal information or images. In the one case in which the House of Lords considered the issue – *Wainwright v Home Office* – it declined to recognise a general right to privacy which would extend to physical privacy interferences such as the intrusive strip search to which prison officers subjected the claimants in that case.[1]

* Associate Professor of Law, Victoria University of Wellington. I would like to thank Mark Warby QC, 5 Raymond Buildings, London; Professor Tanya Aplin, King's College London; Professor John Bell, University of Cambridge; and two anonymous peer reviewers for their helpful comments on earlier drafts. Thanks also to Steven Price, Barrister, Wellington, and participants in a joint meeting of the University of Cambridge Centre for Public Law and Torts Research Group at which an earlier version of this work was presented. I accept full responsibility for all content.

[1] *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406.

There is more to privacy, however, than the unwanted collection and dissemination of private information. Privacy can also be breached by unwanted watching, listening or recording even if little information is obtained and none is disseminated. Peering through a person's bedroom window, following him or her around, bugging his or her home or telephone calls, or surreptitiously taking for one's own purposes an intimate photograph or video recording are all examples of this kind of intrusion. According to some commentators, it is the desire to protect against these interferences which "brings us to the core of our expectations and intuitions about privacy and hence of our rights to it".[2] It is therefore unsurprising that US courts and, recently, both the Ontario Court of Appeal and New Zealand High Court have recognised that a tort is committed if a person intrudes upon "the solitude or seclusion of another or his private affairs or concerns" in circumstances where the "intrusion would be highly offensive to a reasonable person".[3] Law reform bodies, both in England and abroad, have consistently recommended similar protections.[4]

This article asks how effectively English law protects against these non-informational breaches of privacy. More particularly, it asks how English law protects against unwanted watching, listening, and recording and whether and how that protection should be extended. The discussion is divided into four sections. The first section deconstructs the concept of privacy, identifying two main components of the interest – one informational and one physical. The second examines the right to respect for private life in Article 8 of the European Convention for the Protection of Human Rights 1950 (the "Convention") highlighting, in particular, the inclusion of both informational and physical privacy within that interest. Attention then turns to the adequacy of legal protections in English law. A survey is made of existing common law and legislative protections against unwanted observation and recording, including those provided by breach of confidence, misuse of private information, intentional infliction of emotional distress, the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000. This survey shows that protection for physical privacy is currently patchy and uncomprehensive. The article therefore concludes by making the case for recognition of a specific,

[2] T. Gerety, "Redefining Privacy" (1977) 12 Harvard Civil Rights–Civil Liberties Law Review 233, 265.

[3] See the Restatement of the Law Second, Torts 2d (Vol.3), 1976, § 652B; *Jones v Tsige* (2012) ONCA 32, 333 D.L.R. (4th) 566; and *C v Holland* [2012] NZHC 2155, [2012] 3 N.Z.L.R. 672.

[4] See, e.g., M. Littman and P. Carter-Ruck (chairmen), *Privacy and the Law: A Report by Justice* (London 1970), 41–42; K. Younger (chairman), *Report of the Committee on Privacy* (London 1972), at [53]; D. Calcutt (chairman), *Report of the Committee on Privacy and Related Matters* (London 1990), at [17.8]–[17.9]; New South Wales Law Commission, *Report 120: Invasion of Privacy* (Sydney 2009), at [4.3]; Australian Law Reform Commission, *Discussion Paper 80: Serious Invasion of Privacy in the Digital Era* (2014), Proposal 5-1; and New Zealand Law Commission, *Report 113: Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy Stage 3* (Wellington 2010), 3.

narrowly-focussed intrusion tort from within the misuse of private information action.

II. Theoretical Conceptions of Physical Privacy

Case law, scholarly writing and popular discourse abound with stories of people breaching one another's privacy. Analysis of these examples helps us to articulate our intuitive understanding of what privacy is and how it is interfered with. A list of common intrusions is therefore a useful starting point for an examination of the privacy interest.

The first way that X can breach Y's privacy is by obtaining access to private records that Y does not want X to see, such as his or her medical notes, banking details, emails, letters, tax returns or diaries. Secondly, X can breach Y's privacy by enabling others to find out about Y, for example, by uploading Y's personal records to the Internet or publishing a story revealing their content in the newspaper. Alternatively, X could file private material away to be re-examined on some future occasion or, if X is a former confidant, he or she could reveal Y's secrets or talk about intimate experiences they have both shared – X could kiss and tell, pass on a closely-held confidence, or tell the world intimate details of Y's day-to-day life. X could also disseminate consensually-taken images against Y's wishes; images of Y naked or engaged in sexual activity, for instance. In other cases, X might spy on people when they do not want to be seen – when they are using a shower, toilet, or changing room – or eavesdrop when they do not want to be heard, such as when they are talking on the telephone or in the confines of their home. And X could film, photograph or record these private activities with a view either to revisiting them later or sharing them with others – for example, by uploading photographs, videos or audio recordings to the Internet, broadcasting them on television, or publishing them in a newspaper.

Although each of X's privacy breaches is effected differently, they all prevent the subject from choosing, on his or her own terms, the extent to which he or she is accessed by others. All of them – whether they involve disclosure of a secret, publication of a photograph, or voyeuristic spying – also lead to feelings of affront, violation and indignity. To use Stanley Benn's words, individuals in these cases are being treated "as objects or specimens" to be looked at, listened to or found out about at whim, not as "subjects with sensibilities, ends, aspirations of their own".[5] Distress, humiliation and, in some cases, mental harm can result.[6]

[5] S. Benn, "Privacy, Freedom, and Respect for Persons" in J. Pennock and J. Chapman (eds.) *Privacy: NOMOS XIII* (New York 1971), 6–7.

[6] See, for example, *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406, at [4]; the evidence of targets of media "door-stepping" in *AM v News Group Newspapers Ltd.* [2012] EWHC 308 (QB), at [4] and *AAA v Associated Newspapers Ltd.* [2012] EWHC 2103 (QB), at [15]–[16] and [31] (although

It is therefore unsurprising that all of these activities have been held to be part of a right to privacy in at least some common law jurisdictions. In England, it is actionable to kiss and tell, to divulge secrets or other private information, to read or publish information contained in private records and to disseminate photographs or videos of intimate activities.[7] And in other common law jurisdictions, courts have upheld claims against defendants who bug their tenants; spy on people in toilets, showers or changing rooms; disseminate consensually-taken sex tapes to friends and family; or intercept people's telephone calls.[8] Academics have also identified as "typical invasions of privacy":

> the collection, storage, and computerization of information; the dissemination of information about individuals; peeping, following, watching, and photographing individuals; intruding or entering "private" places; eavesdropping, wiretapping, reading of letters; drawing attention to individuals; and forced disclosure of information.[9]

All of these different modes of intrusion interfere with personal privacy. There are, however, important conceptual differences between them which need to be recognised if privacy is to be properly understood. It is suggested, in particular, that the examples listed above reveal two types of overlapping but distinct privacy interference: the misuse of private information (informational privacy) and unwanted sensory access (physical privacy).[10]

the reliability of some witnesses' recollection of events was doubted in the latter case, their evidence about the effect it had upon them was not called into question (see paras. [40]–[49]); and Rt. Hon Lord Justice Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press*, House of Commons Paper No. 780 (London 2012), 484, at [3.4]. Further, the claimant in *C v Holland* [2012] NZHC 2155, [2012] 3 N.Z.L.R. 672 (interviewed by this author and Dr Yvette Tinsley on 27 March 2014) suffered distress and anxiety so acute that she was unable to go out in public for a week after discovering that her flatmate had filmed her in the shower. Other effects such as insomnia, nightmares, mistrust of others, fear of the defendant and feelings of shame continued for months after the discovery of the filming.

[7] See e.g., respectively, *Barrymore v News Group Newspapers Ltd* [1997] F.S.R 600; *McKennitt v Ash* [2006] EWCA Civ 1714; *Associated Newspapers Ltd v HRH Prince of Wales* [2006] EWCA Civ 1776; and *Mosley v News Group Newspapers Ltd.* [2008] EWHC 1777 (QB), [2008] E.M.L.R. 20.

[8] See e.g., respectively, *Amati v City of Woodstock, Illinois* 829 F.Supp. 998 (N.D.Ill 1993); *Harkey v Abate* 346 N.W.2d 74 (Mich.App. 1983); *C v Holland* [2012] NZHC 2155, [2012] 3 N.Z.L.R. 672; *Benitez v KFC National Management* 714 N.E.2d 1002 (Ill.App.2 Dist. 1999); *Giller v Procopets* [2008] VSCA 236 (10 December 2008); and *Rhodes v Graham* 37 S.W.(2d) 46 (1931).

[9] R. Gavison, "Privacy and the Limits of the Law" (1979) 89 Yale L.J. 421, 436. See also Daniel Solove's broad taxonomy in "A Taxonomy of Privacy" (2006) 154 U. Pa. L. Rev. 447.

[10] For a fuller development of this argument, see N. Moreham "The Protection of Privacy in English Common Law: A Doctrinal and Theoretical Analysis" (2005) 121 L.Q.R. 628. Many academics divide the concept along similar lines. See, e.g., Gavison, note 9 above, at pp. 428–40; Solove, note 9 above, at p. 489ff; T. Gerety, note 2 above, p. 261ff; S. Benn, note 5 above, pp. 3–4; J. Rachels, "Why Privacy is Important" (1975) 4 Phil. & Publ. Aff. 323, 326; J. Wagner De Cew, "The Scope of Privacy in Law and Ethics" (1986) 5 L. & Phil. 145, 153–58; E. van den Haag, "On Privacy" in J. Pennock and J. Chapman (eds.), *Privacy: NOMOS XIII* (New York 1971), 149, 149–53; R. Mulheron, "A Potential Framework for Privacy? A Reply to *Hello!*" (2006) 69 M.L.R. 679, 696–701; C. Hunt, "Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort" (2011) 37 Queen's L.J. 167, 201; R. Wacks, *Privacy and Media Freedom* (Oxford 2013), ch. 6; and K. Hughes, "A Behavioural Understanding of Privacy and its Implications

The principal objection in the informational privacy cases is to the fact that someone is *finding out* something about you against your wishes. He or she is learning that you have a sexually-transmitted infection, that you enjoy cross-dressing in private, that you run your home in a particular way, that you are having relationship difficulties, or that you are the anonymous author of a popular blog. These informational privacy interferences, in turn, take three main forms. First, a person can breach your informational privacy by *discovering* things about you that you wish to keep to yourself (by acquiring your bank records, reading your diaries, or hacking your emails, for instance). Secondly, he or she can *retain* private records or information about you either for his or her own future reference or with a view to sharing the information with others (by building up a computer file or secret dossier, for example). And, thirdly, the person can *disclose* private information about you to others, by passing on gossip, uploading facts, photographs or other material to the Internet, or disseminating it in the media.[11] It follows that many of the examples outlined above fall within the informational privacy category – kissing and telling, reading somebody's personal records, uploading them to the Internet, assembling a secret dossier, and disseminating photographs or other recordings are all examples of this kind of interference.

The second category – physical privacy – is all about unwanted access to the physical self. The interference in these cases is *sensory*: the intruder interferes with your physical privacy by watching, listening to or otherwise sensing you against your wishes.[12] It is this aspect of the interest which is at stake when X spies on Y in the shower, hacks Y's telephone calls, or videos Y in his or her bedroom. And this physical privacy interest can, again, be interfered with in three main ways. It is a breach of your physical privacy, first, to *observe* you against your wishes (including with technological aids), for instance, by spying on you as you get changed, filming you in the bathroom, or bugging you during an intimate telephone call. Secondly, physical privacy is compromised when a person *photographs or otherwise records* your private activities.[13] And finally, it is a breach of physical privacy to enable others to see or hear you engaged in private activities by *disseminating photographs or recordings* of those activities to

for Privacy Law" (2012) 75 M.L.R. 806, 810–11. See also R. Parker, "A Definition of Privacy" (1974) 27 Rutg. L. Rev. 275, 275–88.

[11] Daniel Solove divides informational privacy into similar categories – information collection, information processing, and information dissemination – although his conception of the privacy interest is broader than the one offered here: see Solove, note 9 above, at p. 489ff.

[12] This definition of physical privacy is narrower than the concept of intrusion promulgated in the Restatement of the Law Second, Torts 2d (Vol.3), 1976, § 652B; *Jones v Tsige* (2012) ONCA 32, 333 D.L.R. (4th) 566; *C v Holland* [2012] NZHC 2155, [2012] 3 N.Z.L.R. 672; *Goodwin v MGN Ltd.* [2011] EWHC 1437 (QB), [2011] E.M.L.R. 27, at [85]–[130]; *CBT v News Group Ltd.* [2011] EWHC 1326 (QB), at [23]–[26]; and by commentators such as Solove, note 9 above, at p. 552; Wacks, *Privacy and Media Freedom*, note 10 above, ch. 6.

[13] This is because recording facilitates further sensory perception by those with access to the recording.

others. In all of these situations, the concern is primarily physical: the observer is, through the use of the senses, physically experiencing something of you against your wishes and/or allowing others to do the same.

There is, of course, overlap between the two categories. A person who hacks another's telephone will obtain sensory access to the speakers and, sometimes also information about private matters. Likewise, a landlord who installs a camera in his or her tenant's bathroom will find out what the tenant does there as well as seeing him or her naked. Nonetheless, both these components of the privacy interest – physical and informational – need to be recognised if privacy is to be comprehensively protected. This is because it is possible to commit a serious breach of privacy without obtaining any meaningful information. Little "information" is obtained, for example, when a person is spied on in the shower, bugged having an anodyne conversation in his or her bedroom, watched in a toilet, or videoed whilst having a shower. Further, even if some meaningful information is obtained, it is unlikely to be the sole reason for the subject's objection. As Raymond Wacks has said:

> What is essentially in issue in cases of intrusion is the frustration of the legitimate expectations of the individual that he should not be seen or heard in circumstances where he has not consented to or is unaware of such surveillance. The quality of the information thereby obtained, though it will often be of an intimate nature, is not the major objection.[14]

Thus, a person watching a surreptitiously-obtained video of a woman giving birth, not only obtains medical information about her, he *sees* intimate parts of her body, *hears* her crying out and generally insinuates himself into an intimate occasion.[15] All these aspects of the interest need to be vindicated if the woman's privacy is to be protected. A notion of privacy which focussed just on the information obtained – about the nature of the labour, the interventions received and the medical decisions made – would only tell half the story.

It follows that conceptions of privacy which, like the current English common law, focus exclusively on the acquisition or dissemination of private information, fail to accommodate physical privacy interests effectively.

III. Physical Privacy in Strasbourg

This two-part – physical and informational – conception of the privacy interest is consistent with Strasbourg's articulation of the right to respect

[14] R. Wacks, *Personal Information: Privacy and the Law* (Oxford 1989), 248. See also Wacks, *Privacy and Media Freedom*, note 10 above, pp. 120–22; 186–219.
[15] See *De May v Roberts* (1881) 46 Mich. 160, 9 N.W. 146.

for private life in Article 8 of the Convention.[16] Numerous decisions of the European Court of Human Rights confirm that it is an interference with Article 8(1) not only to publish private information but also to collect or store it, even if it is not subsequently used or disseminated.[17] In addition, "private life" encompasses wide-ranging protection of an individual's "physical and psychological integrity" and a right to "personal development".[18] These concepts extend to many of the physical intrusions discussed above, including intrusive body searching, search of residential or work premises, and surveillance or recording in, for example, a person's home, garage or prison cell.[19]

The European Court has also expressly recognised positive obligations on Member States to protect citizens from unwanted photography and video surveillance. In the recent case of *Söderman v Sweden*, the Grand Chamber held that Sweden breached its positive obligations to a 14-year-old girl by failing to provide civil or criminal sanction against her step-father after he surreptitiously filmed her changing in the bathroom.[20] This is consistent with the First Chamber's decision, in *Reklos and Davourlis v Greece*, that Greek domestic courts failed to protect the private life interests of a day-old child who was photographed without his parents' consent whilst in a sterile unit in hospital, even though there was no suggestion that the photographs had been or were to be disseminated.[21] The court in that case said that:

> Whilst in most cases the right to control [the use of one's image] involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the *recording, conservation and reproduction of the image* by another person. As a person's image is one of the characteristics attached to his or her personality, its effective protection presupposes, in principle and in circumstances such as those of the present case …

[16] Article 8 provides that: "(1) Everyone has the right to respect for his private life 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".

[17] See, e.g., *Leander v Sweden* (Application no. 9248/81) (1987) 9 E.H.R.R. 433, at [48]; *Rotaru v Romania* (Application no. 28341/95) (2000) 8 BHRC 449, at [44]; and *Segerstedt-Wiberg v Sweden* (Application no. 62332/00) (2007) 44 E.H.R.R. 2, at [72]–[73].

[18] See, respectively, *Pretty v United Kingdom* (Application no. 2346/02) (2002) 35 E.H.R.R. 1, at [61]; and *YF v Turkey* (Application no. 24209/94) (2004) 39 E.H.R.R. 34, at [33]; and *Peck v United Kingdom* (Application no. 44647/98) (2003) 36 E.H.R.R. 41, at [57].

[19] See, respectively, *Wainwright v United Kingdom* (Application no. 12350/04) (2007) 44 E.H.R.R. 40 and *Gillan and Quinton v United Kingdom* (Application no. 4158/05) (2010) 50 E.H.R.R. 45; *Funke v France* (Application no. 10828/84) (1993) 16 E.H.R.R. 297; *Chappell v United Kingdom* (Application no. 10461/83) (1989) 12 E.H.R.R. 1; *Chalkley v United Kingdom* (Application no. 63831/00) (2003) 37 E.H.R.R. 30; *Hewitson v United Kingdom* (Application no. 50015/99) (2003) 37 E.H.R.R. 31; and *Perry v United Kingdom* (Application no. 63737/00) (2004) 39 E.H.R.R. 3.

[20] *Söderman v Sweden* (Application no. 5786/08), Judgment of 12 November 2013, not yet reported, at [117].

[21] *Reklos and Davourlis v Greece* (Application no. 1234/05) (2009) E.M.L.R 16.

> obtaining the consent of the person concerned *at the time the picture is taken and not simply if and when it is published*. Otherwise an essential attribute of personality would be retained in the hands of a third party and the person concerned would have no control over any subsequent use of the image.[22]

In other words, the disclosure of private material is not a prerequisite for an Article 8 claim: physical intrusion effected by filming, photographing or recording is in some circumstances actionable per se.

The broad scope of the Article 8 right to private life articulated in Strasbourg case law reinforces the view that privacy (which is closely related to private life) includes protection of both physical and informational privacy interests. It also has direct implications for the development of English private law. As a signatory to the Convention, the United Kingdom has (in addition to its negative obligation to avoid breaching Article 8) a positive obligation to protect citizens against Article 8 interferences by private actors. As the Grand Chamber has recently confirmed, this obliges Member States to "maintain and apply in practice an adequate legal framework affording protection" of a citizen's private life rights.[23] The nature of the State's obligation "will depend on the particular aspect of private life that is at issue"[24] but the Member State must provide, as a minimum, some kind of civil protection against the interference in question.[25] As just discussed, the European Court has already found that, in at least some circumstances, failure to protect against unauthorised photography and surreptitious filming by private actors breaches these obligations. There is no obvious reason why private acts of surveillance or recording by other means (audio recording or telephone hacking, for example) should be treated any differently.

In addition, and partly in response to the United Kingdom's positive obligations under the Convention,[26] English domestic courts have recognised the horizontal effect of Article 8 of Schedule 1 to the Human

[22] Ibid., at para. [40] (emphasis added). The court also took account of the fact that the photographs were taken in a place that was accessible only to the doctors and nurses of the clinic (at para. [37]); that the baby's image was the sole subject of the photographs (at para. [37]); there was no public interest in the baby (at para. [41]); that the parents did not consent to the photography (at para. [41]); and that the photographer retained the negatives (at para. [42]). For a useful critique of the court's reasoning see K. Hughes, "Photographs in Public Places and Privacy" [2009] 2 J.M.L. 159, 163–68.

[23] *Söderman v Sweden* (Application no. 5786/08), Judgment of 12 November 2013, not yet reported, at [85].

[24] Ibid., at [79] and *von Hannover v Germany (No. 2)* (Application no. 40660/08 and 60641/08) (2012) 55 E.H.R.R. 15, at [104]. The Grand Chamber has reiterated, however, that the court's task is not to "take the place of the national courts" but to review whether the decisions taken are compatible with the provisions of the Convention relied on (*von Hannover v Germany (No. 2)* (Application no. 40660/08 and 60641/08) (2012) 55 E.H.R.R. 15, at [105] and *Axel Springer AG v Germany* (Application no. 39954/08) (2012) 55 E.H.R.R. 6, at [86]).

[25] *Söderman v Sweden* (Application no. 5786/08), Judgment of 12 November 2013, not yet reported, at [85].

[26] See, e.g., *Douglas and others v Hello! Ltd* [2000] EWCA Civ 353, [2001] Q.B. 967 (CA), at [111] (per Sedley L.J.).

Rights Act 1998 (the "HRA"). Although the HRA only has direct effect in disputes between citizen and the state, courts have, for a variety of reasons, held themselves bound to act consistently with the Convention when developing the common law.[27] This horizontal effect does not create new causes of action between private persons but obliges courts to develop any "applicable" causes of action consistently with Convention principles.[28] The exact scope of this obligation remains unclear but it is perhaps best articulated as a duty to "in so far as possible, develop the common law in such a way as to give effect to Convention rights".[29] In other words, as Gavin Phillipson and Alexander Williams put it, "the courts must develop the common law compatibly with the Convention, but only where such development can be achieved by 'incremental' development".[30]

All this means that English courts should incrementally develop the common law to protect private life interests identified in Strasbourg. Those rights include the right to be free from unjustified surveillance, search, and recording.[31] This, as will be discussed below, has significant implications for the protection of physical privacy in English private law.

IV. Physical Privacy in English Law: The Gaps in Protection

So, physical privacy is an essential part of both theoretical conceptions of privacy and the Article 8 right to private life. It follows that if English law is to protect privacy comprehensively, both physical and informational privacy need to be protected. The House of Lords' decision in *Wainwright v Home Office* that there is no general right to privacy in English law means that there is no all-encompassing common law action which does this. Lord Hoffmann, with whom other members of the House concurred, said that although privacy values might underpin common law actions such as breach of confidence, recognition of a "high-level principle" of privacy was neither desirable nor necessary to comply with the

[27] Courts, as "public authorities", have held themselves bound by section 6 of the Human Rights Act 1998 ("HRA") to act consistently with Convention principles (see *Douglas and others v Hello! Ltd* [2000] EWCA Civ 353, [2001] Q.B. 967 (CA), at [111] (per Sedley L.J.) and [166] (per Keene L.J.); *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] A.C. 457, at [114] (per Lord Hope) and [132] (per Baroness Hale)). Reference has also been made to the United Kingdom's positive obligations (ibid.) and the enactment of section 12(4) of the HRA (*Douglas and others v Hello! Ltd* [2000] EWCA Civ 353, [2001] Q.B. 967 (CA), at [92]–[95] (per Brooke L.J.) and [133] (per Sedley L.J.).

[28] *Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [132] (per Baroness Hale).

[29] *HRH Prince of Wales v Associated Newspapers* [2006] EWCA Civ 1776, [2008] Ch. 57, at [25] (per Lord Phillips MR, speaking for the court). See also *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] A.C. 457, at [17] (per Lord Nicholls) and [132] (per Baroness Hale).

[30] G. Phillipson and A. Williams "Horizontal Effect and the Constitutional Constraint" (2011) 74 M.L.R. 878, 878-79. See also M. Hunt "The Horizontal Effect of the Human Rights Act" [1998] P.L. 423, especially 441–42; and A. Lester and D. Pannick "The Impact of the Human Rights Act on Private Law: The Knight's Move" (2000) 116 L.Q.R. 380.

[31] See, e.g., *Mosley v News Group Newspapers Ltd.* [2008] EWHC 1777 (QB), [2008] E.M.L.R. 20, at [103]–[104] in which Eady J. took account of Strasbourg cases on surveillance and clandestine recording when deciding that the claimant had a reasonable expectation of privacy.

United Kingdom's obligations under the Convention.[32] Privacy protection, then, has had to develop incrementally. In order to articulate the scope of privacy protection in English law, one therefore has to examine a range of legislative protections and common law actions. This section does that, asking how effectively those various measures protect informational and physical privacy and identifying the gaps that remain.

A. The Scope of Breach of Confidence and Misuse of Private Information

As is well known, the breach of confidence action has been the main vehicle for the development of English privacy rights. But how far has that vehicle taken us towards comprehensive privacy protection.

The breach of confidence action traditionally focussed on the wrongful disclosure of – usually commercial – information which had been voluntarily divulged to the defendant.[33] Continuous development of its requirements meant, however, that by the end of last century, duties of confidence could attach to personal as well as commercial information[34] and to information which was not divulged but deliberately, or even adventitiously, taken.[35] These developments, bolstered further by the horizontal effect of Article 8 of Schedule 1 to the HRA, eventually led to the emergence of a specific informational privacy action.[36] The touchstone of this new action – labelled "misuse of private information" – is whether the person in question had a reasonable expectation of privacy in respect of the disclosed facts.[37] This question has, in turn, been incorporated into a "new methodology" under which courts ask, first, whether Article 8 is "engaged" (determined by applying the reasonable expectation of privacy test just outlined) and if so, whether the Article 8 interest in privacy should yield to the defendant's Article 10 right to freedom of expression.[38]

As with breach of confidence, the primary concern of the misuse of private information action is the unwanted disclosure of private information.[39]

[32] *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406, at [18] and [31]–[32].

[33] For discussion of the development of the action see *Tchenguiz v Imerman* [2010] EWCA Civ 908, at [54]–[71].

[34] See, e.g., *Duchess of Argyll v Duke of Argyll and others* [1967] 1 Ch. 302 and *Stephens v Avery* [1988] 1 Ch. 449.

[35] See, e.g., *Francome and another v Mirror Group Newspapers Ltd. and others* [1984] 1 W.L.R. 892; *Shelley Films Ltd. v Rex Features Ltd.* [1994] E.M.L.R. 134; *Creation Records and others v News Group Newspapers Ltd.* [1997] E.M.L.R. 444; and *Attorney-General and Observer Ltd. v Times Newspapers Ltd.* [1990] 1 A.C. 109, 281.

[36] See *Douglas and others v Hello! Ltd* [2000] EWCA Civ 353, [2001] Q.B. 967 (CA), especially [111] (per Sedley L.J.).

[37] *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [14] and [21] (per Lord Nicholls). See also ibid., at [96] (per Lord Hope) and [134] (per Baroness Hale).

[38] See, e.g., *McKennitt v Ash* [2006] EWCA Civ 1714, [2008] Q.B. 73, at [11] and *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [17]-[21].

[39] All the tests in the leading case of *Campbell v MGN Ltd.* refer to the dissemination of information (see *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [21] (per Lord Nicholls), [92] (per Lord Hope) and [134]) (per Baroness Hale).

The action therefore protects against disclosure of facts about a person's private life (the details of an extra-marital affair or drug addiction treatment, for example)[40] and against disclosure of private "information" contained in photographs or other recordings of private activities (such as sexual activities or family outings).[41] With regard to the latter, courts have recognised that publication of such images can intrude into private life "in a peculiarly humiliating and damaging way",[42] but no protection is given against the *making* of a photograph or other recording without subsequent publication.[43] So, although misuse of private information protects against the third of both the informational and physical privacy categories identified above – the disclosure of private information and of photographs or other recordings, respectively – it does not protect against the act of recording.

The relationship between "traditional" breach of confidence and the new action for misuse of private information is not entirely clear, but the latest Court of Appeal authority, *Tchenguiz v Imerman*, confirms that breach of confidence operates alongside misuse of private information and provides an alternative avenue for redress if the traditional requirements of breach of confidence are met.[44] The significance of this alternative option for redress has been greatly enhanced by an expansive interpretation, in *Tchenguiz*, of the requirement that the information be "misused" by the defendant.[45] The defendants in that case were concerned that the claimant was hiding his assets from their sister, with whom he was engaged in matrimonial proceedings. To thwart these attempts, the defendants accessed, copied and passed on to their sister's solicitor, documents which the claimant kept on a computer server in their shared office. The Court of Appeal held that obtaining the information, without more,

[40] See, e.g., *CBT v News Group Newspapers Ltd* [2011] EWHC 1232 (QB); *Goodwin v MGN Ltd.* [2011] EWHC 1437 (QB), [2011] E.M.L.R. 27; and *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457.

[41] See, respectively, *Theakston v Mirror Group Newspapers Ltd.* [2002] EWHC 137 (QB), [2002] E.M.L.R. 22 and *Mosley v News Group Newspapers Ltd.* [2008] EWHC 1777 (QB), [2008] E.M.L.R. 20; and *Murray v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch. 481.

[42] *Theakston v Mirror Group Newspapers Ltd.* [2002] EWHC 137 (QB), [2002] E.M.L.R. 22, at [78]. See also *Douglas and others v Hello! Ltd* [2000] EWCA Civ 353, [2001] Q.B. 967 (CA), at [165]; *Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [72]; *D v L* [2003] EWCA Civ 1169, [2004] E.M.L.R. 1 at [23]; and *Douglas v. Hello! Ltd. (No. 6)* [2005] EWCA Civ 595, [2006] Q.B. 125, at [106].

[43] *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [122] (per Lord Hope).

[44] *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [66]–[67]. This is consistent with the Court of Appeal's approach in *Associated Newspapers Ltd. v HRH Prince of Wales* [2006] EWCA Civ 1776, [2008] Ch. 57; but, compare *McKennitt v Ash* [2006] EWCA Civ 1714, [2008] Q. B. 73 and *Lord Browne of Madingley v Associated Newspapers Ltd.* [2007] EWCA Civ 295, [2008] 1 Q.B. 103. For further discussion, see N. Moreham, "Breach of confidence and misuse of private information: how do the two actions work together?" (2010) 15 M.A.L.R. 265.

[45] "Misuse" has traditionally involved something more than access to confidential information, such as disclosure to a third party or unauthorised exploitation of trade secrets. See T. Aplin, L. Bently, P. Johnson and S. Malynciz, *Gurry on Breach of Confidence: The Protection of Confidential Information* 2nd ed. (Oxford 2012) at [15.02] and [15.18]–[15.23].

was enough to breach the confidence of the defendant. Speaking for the court, Lord Neuberger M.R. said:

> intentionally obtaining information [in respect of which the defendants must have appreciated that the claimant had an expectation of privacy] secretly and knowing that the claimant reasonably expects it to be private, *is itself* a breach of confidence. The notion that looking at documents which one knows to be confidential is itself capable of constituting an actionable wrong (albeit perhaps only in equity) is also consistent with the decision of the Strasbourg court that monitoring private telephone calls can infringe the Article 8 rights of the caller: see *Copland v United Kingdom* … In our view, it would be a breach of confidence for a defendant, without the authority of the claimant, to examine, or to make, retain, or supply copies to a third party of, a document whose contents are, and were (or ought to have been) appreciated by the defendant to be, confidential to the claimant.[46]

The claimant was therefore able to restrain the defendants from looking at the documents again even though there was no evidence that they intended to reveal the contents to any third party.[47]

This conclusion means that the first and second informational intrusions identified above – the discovery and retention of private information – are also covered by breach of confidence. It is clear from *Tchenguiz* that the acts of acquiring the information and copying/retaining the documents were enough on their own to establish an obligation of confidence, even if no further use was made of the material. It follows that in England, repeatedly accessing (but not disseminating) the banking records of one's partner's former wife, as the bank clerk did in the Ontarian intrusion case of *Jones v Tsige*, would be a breach of confidence.[48]

It follows that common law protection of informational privacy is reasonably comprehensive. All of the informational privacy intrusions identified above – discovering private information, retaining it and disseminating it – potentially fall within the actions for breach of confidence, misuse of private information or both. Both actions also provide redress for the dissemination of photographs, videos or other recordings of a person engaged in private activity, i.e. the third of the physical intrusions identified above.[49]

[46] *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [68]–[69] (emphasis added) citing *Copland v United Kingdom* (Application no. 62617/00) (2007) E.H.R.R. 37.

[47] *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [72].

[48] *Jones v Tsige* (2012) ONCA 32, 333 D.L.R. (4th) 566. For discussion of this case, see T. Bennett, "Privacy, Corrective Justice, and Incrementalism: Legal Imagination and the Recognition of a Privacy Tort in Ontario" (2013) 59 McGill L.J. 49.

[49] Breach of confidence cases involving the disclosure of photographs include *Shelley Films Ltd v Rex Features Ltd* [1994] E.M.L.R. 134 and *Creation Records and others v News Group Newspapers Ltd* [1997] E.M.L.R. 444. See also *Douglas and others v Hello! Ltd* [2000] EWCA Civ 353, [2001] Q.B. 967 (CA), at [113]–[127] (per Sedley L.J.). Some protection against the collection, storage and dissemination of private information (including photographs) is also provided by legislation such as the Regulation of Investigatory Powers Act 2000 ("RIPA"), the Computer Misuse Act 1990 and the Data Protection Act 1998 ("DPA"). However, since comprehensive protection of these informational

Neither breach of confidence nor misuse of private information, though, protects against the non-disclosure aspects of physical privacy. The remainder of this section will look at whether these intrusions – unwanted watching, listening and recording – are actionable elsewhere in English law or whether, as suggested above, there is indeed a gap in current privacy protection.

B. Intentional Infliction of Emotional Distress

So, is there any other common law action which effectively protects against unwanted watching, listening and recording in the absence of actual or threatened dissemination of private material? On first appearances, the tort of intentional infliction of emotional distress is well placed to provide such protection. The action is unconstrained by the information/disclosure focus of breach of confidence and misuse of private information, focussing instead on the distressing and harmful effects of a defendant's conduct. This is precisely the thing at stake when unwanted observation or recording occurs. A closer look at the requirements of intentional infliction of emotional distress, however, reveals a number of limitations.[50]

In *Wilkinson v Downton*, the case in which intentional infliction of emotional distress was established, the claimant suffered "a violent shock to her nervous system" after a practical joker told her that her husband had broken both his legs and was lying injured waiting for her to fetch him.[51] Finding that the claimant had a cause of action against the defendant, Wright J said:

> The defendant has, as I assume for the moment, wilfully done an act calculated to cause physical harm to the plaintiff – that is to say, to infringe her legal right to personal safety, and has in fact thereby caused physical harm to her. That proposition without more appears to me to state a good cause of action, there being no justification alleged for the act. This wilful injuria is in law malicious, although no malicious purpose to cause the harm which was caused nor any motive of spite is imputed to the defendant.[52]

Two requirements emerge from this judgment. This first is that the act was "calculated" or "intended" to cause physical harm. The second is that the claimant suffered actual damage in the form of physical harm or a recognised psychiatric illness. Courts applying the first element do not require proof of actual intention or calculation; an intention to produce the harm will be imputed if the defendant intended to do an act which was

privacy interests is provided by the common law, these additional avenues of redress will not be discussed here.

[50] Raymond Wacks also recognises that the action has some limited potential to protect against intrusion: see Wacks, *Privacy and Media Freedom*, note 10 above, pp. 205–11.

[51] *Wilkinson v Downton* [1897] 2 Q.B. 57, 58.

[52] Ibid., at pp. 58–59.

"sufficiently likely" to lead to the harm suffered.[53] And this test is usually expressed objectively so the defendant will be liable if he or she intended to do an act which could obviously lead to the physical harm which was suffered.[54]

So might there be some physical privacy situations in which both *Wilkinson v Downton* requirements will be met? It might be possible, in some circumstance to impute an intention to cause harm against a person who instals a listening device in his or her tenant's bedroom, films his or her work colleagues getting changed, follows his or her ex-partner around for days, or films his or her neighbours' children in their bedrooms. And such conduct might occasionally lead to physical harm as stipulated by the second requirement: post-traumatic stress disorder, depression, anxiety or paranoia are all potential responses to intrusions of this nature.[55]

But physical privacy cases in which the requirements of *Wilkinson v Downton* are satisfied will be rare. It would be difficult, for example, to establish even an imputed intention to cause harm if the defendant intended his or her intrusion to remain undetected – it is difficult to say that the defendant's spying would "obviously" lead to physical harm when, if it had been up to the defendant, the claimant would have known nothing about it. Further, some judges have held that an intention to cause physical harm should only be imputed if the defendant actually *knew* that such harm was likely to result from his or her conduct.[56] On this subjective approach, an insensitive or unintelligent intruder could escape liability for even the most egregious intrusion simply by failing to consider the impact of his or her actions. The harm requirement is also problematic. Feelings of humiliation, indignity, distress and mistrust are typical consequences of breaches of privacy effected by unwanted observation and recording. Whilst harmful to one's peace of mind, relationships, and sense of self – and, therefore, worthy of compensation in their own right – they do not in themselves amount to physical injury as required by *Wilkinson v Downton*.

[53] See *Wong v Parkside Health NHS Trust* [2001] EWCA Civ 1721, [2003] 3 All E.R. 932, at [12]; *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406, at [44]; and *Wilkinson v Downton* [1897] 2 Q.B. 57, at 59.

[54] See *Wilkinson v Downton* [1897] 2 Q.B. 57, 59 and *Wong v Parkside Health NHS Trust* [2001] EWCA Civ 1721, [2003] 3 All E.R. 932, at [12] (although immediately after her exposition of the objective version of the test, Hale L.J. cited with approval a passage from *Khorasandjian v Bush* [1993] Q.B. 727 supporting a subjective formulation (at [12])). See also *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406, at [44]–[45], where Lord Hoffmann made it clear that the claimant is not required to show that the defendant "acted in a way which he knew to be unjustifiable and either intended to cause harm or at least acted without caring whether he caused harm or not".

[55] In *Wainwright*, Lord Woolf C.J. held that the claimants – who respectively experienced exacerbation of an existing depressive condition and post-traumatic stress disorder following an invasive strip search during a prison visit – had suffered damage which was capable of sustaining a *Wilkinson v Downton* claim (*Wainwright v Home Office* [2001] EWCA Civ 2081, [2002] Q.B. 1334, at [51]).

[56] See the headnote to *Janvier v Sweeney* [1919] 2 K.B. 316 adopted by the majority of the Court of Appeal in *Khorasandjian v Bush* [1993] Q.B. 727, 735 and *Wainwright v Home Office* [2001] EWCA Civ 2081, [2002] Q.B. 1334, at [79] (per Buxton L.J.).

It follows that intentional infliction of emotional distress could only provide comprehensive protection against unwanted observation and recording – and hence plug the physical privacy gaps under discussion – if its requirements were substantially relaxed. Courts would need to abandon the requirement of intention (or at least favour an objective, over a subjective, approach) and allow recovery for distress and upset falling short of physical harm. There is perhaps an argument that the courts' obligation to develop the common law consistently with Article 8 would now justify extensions of this nature: as in breach of confidence, this argument would go, courts are obliged to develop *Wilkinson v Downton* incrementally to protect physical privacy interests.[57]

The trend, however, is not in that direction. Lord Hoffmann showed some willingness to relax the physical injury requirement when he said, in *Hunter v Canary Wharf*, that he saw "no reason why a tort of intention should be subject to the rule which excludes compensation for mere distress, inconvenience or discomfort in actions based on negligence".[58] But the injury requirement has been confirmed by superior courts on numerous occasions[59] and Lord Hoffmann read down his own comments when he revisited the issue in *Wainwright*.[60] Further, as outlined above, some judges support a narrower, not broader, reading of the intention component and therefore require actual knowledge of the likelihood of harm. The general approach has therefore been to regard *Wilkinson v Downton* as an anomaly in the law of torts and to read its requirements accordingly.[61] It seems unlikely then, even in the post-HRA context, that courts would be willing to make the significant extensions required to turn intentional infliction of emotional distress into a useful physical privacy action. Claimants seeking redress for physical privacy interferences should therefore pursue other, more favourable, options.

C. Legislative Protections

So, there is no clear common law right protecting against unwanted observation and recording where subsequent dissemination of material has not occurred. The final question for this section is whether legislative measures fill that gap.

[57] See "Physical Privacy in Strasbourg" above. The fact that all the leading *Wilkinson v Downton* cases pre-dated the application of the HRA might provide some support for this argument.

[58] *Hunter v Canary Wharf* [1997] A.C. 655, 707.

[59] *Wong v Parkside Health NHS Trust* [2001] EWCA Civ 1721, [2003] 3 All E.R. 932, at [11]–[12]; *Wainwright v Home Office* [2001] EWCA Civ 2081, [2002] Q.B. 1334 (CA), at [47]–[49] (per Lord Woolf CJ); and *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406, at [47] (per Lord Hoffmann).

[60] *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406, at [44]–[46] (per Lord Hoffmann). See also para. [62] (per Lord Scott).

[61] See, for example, Lord Hoffmann's observations about the, somewhat unprincipled, reasons for the action's inception (ibid., at para. [44]).

There is no doubt that the importance of physical privacy has been recognised by the legislature. Numerous legislative measures provide some protection against unwanted watching, listening and audio and visual recording. Section 67 of the Sexual Offences Act 2003 ("SOA"), for example, makes it an imprisonable offence to observe and/or record for sexual gratification a person doing a private act, knowing that he or she does not consent to being observed for that purpose.[62] In addition, the Protection from Harassment Act 1997 ("PHA") creates civil and criminal liability for stalking and shadowing, spying, unwanted photography and video recording which form part of a harassing course of conduct;[63] the Regulation of Investigatory Powers Act 2000 ("RIPA") prohibits interception of telephone calls or messages awaiting collection;[64] and the Data Protection Act 1998 ("DPA") protects against, inter alia, observation or recording with digital devices.[65]

There is no legislative measure, however, which comprehensively protects against unwanted watching, listening or recording in all circumstances. The PHA, for example, only protects against physical intrusion if it forms part of a "course of conduct" which means that there must have been harassing behaviour on at least two occasions.[66] Similarly, the SOA voyeurism offence is only committed if the person spied on was using a toilet, engaged in sexual activity or had intimate body parts exposed and the prosecution can establish a sexual motivation. An individual who spied on a person in a toilet out of spite, curiosity, artistic interest, suspicion of malpractice, or even a desire to blackmail could therefore avoid a voyeurism conviction.[67] And, although at first glance the provisions of the DPA seem far-reaching, they do not apply to the use of non-digital recording or surveillance devices, to people gathering data for the "special purposes" of journalism, art or literary endeavour (at least as far as the

[62] Sexual Offences Act 2003, s. 67. The sexual gratification can either be one's own (s. 67(1)) or, if the recording was made to facilitate another's observation, someone else's (ss. 67(2) and (3)).

[63] See, respectively, *Howlett v Holding* [2006] EWHC 41 (QB), at [24]; *R* v. *Hayes* [1999] 3 All ER 816; *Crawford v CPS* [2008] EWHC 148 (Admin); and *King v DPP* (Unreported, Divisional Court, Kennedy L.J. and Jackson J., 20 June 2000). Since November 2012, "stalking" has also been a specific offence (see Protection from Harassment Act 1997 ("PHA"), ss. 2A and 4A). Harassing conduct is punishable with a fine, imprisonment for up to six months, and/or restraining order (see PHA, ss. 2 and 5 respectively).

[64] RIPA, ss. 1(1) and (2) and 2(7). This includes messages on the voicemail facility of a public telecommunications system which have already been accessed by the recipient (*Coulson v Regina* [2013] EWCA Crim 1026).

[65] See *Douglas v Hello! Ltd. (No. 6)* [2003] EWHC 786 (Ch), [2003] 3 All E.R. 996, at [230]; and *Douglas and others v Hello! Ltd* [2000] EWCA Civ 353, [2001] Q.B. 967 (CA), at [55]–[56]. For a complete survey of legislative protection against physical intrusion in English law, see N. Moreham "Protection against Intrusion in English Legislation" in N. Witzleb, D. Lindsay, M. Paterson and S. Rodrick (eds.) *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge 2014).

[66] PHA, ss. 1 and 7(3). See also *Majrowski v Guy and St Thomas's N.H.S. Trust* [2006] UKHL 34, [2007] 1 AC 224, at [66] (*per* Baroness Hale).

[67] See *R v Henderson* [2006] EWCA Crim 3264, at [10] in which the defendant claimed, albeit unsuccessfully, that his interest in women urinating was "visual" rather than sexual.

Privacy Principles and protections against distress are concerned),[68] nor to data being processed for the purposes of "personal, family or household affairs (including recreational purposes)".[69] And, no offence is committed under RIPA if a person installs a listening device outside the telecommunications network, in the home or car of another or on the outside of a telephone, for example.[70]

Even when considered collectively, legislative protection of physical privacy is uncomprehensive. To take visual recording as an example, filming a person who is engaged in an intimate act or in a state of undress can be criminal but defendants will escape liability if, inter alia, their motive was not sexual. Perpetrators could also fall foul of the DPA but not if they used a non-digital filming device or made the film for their own domestic purposes. The PHA will not apply if the filming was a one-off event. Protection against eavesdropping is similarly patchy.[71]

All this means that there is no obvious criminal or civil sanction against an individual who, for his or her own recreational purposes, videos his or her tenants in their living room, films the neighbours' children in their bedrooms, installs bugging devices in a former friend's car, or films his or her ex-spouse in the toilet in case he or she wants to use the footage for blackmail on some future occasion. Even where criminal sanction exists, it is rare to find corresponding civil liability. This means that, often, victims are inadequately compensated for the distress and harm caused by the intrusion. And, of course, except in the unusual case of a private prosecution, criminal sanction depends on police willingness to investigate and prosecute. The tabloid telephone hacking scandal has infamously shown that this is a process over which victims have little control.

V. Filling the Gaps: Enhancing Protection Against Unwanted Observation and Recording

Current legal protections against unwanted watching, listening and recording are therefore inadequate. There would be no clear basis in English law for compensating the claimant in *C v Holland* who suffered significant

[68] DPA, s. 32(1) and (2) (Privacy Principle 7, which relates to data security, is exempted).

[69] DPA, s. 36.

[70] See, for example, *R v E* [2004] EWCA Crim 1243, [2004] 1 WLR 3279, at [20] (no "interception" when a listening device in the defendant's car picked up just his end of a conversation on a mobile telephone); *R v Smart* [2002] EWCA Crim 772, [2002] Crim LR 684, at [68] (in which the same conclusion was reached under the Interception of Communications Act 1985 (UK)); and *R v Hardy* [2002] EWCA Crim 3012, [2003] 1 Cr. App. R. 30, at [31] (no interception where an undercover police office recorded his end of a telephone call). See also RIPA, s. 2(2).

[71] It is criminal to intercept a private conversation on the telecommunications network but not to bug a conversation outside it (although if the bugging occurred on a private telephone network there is a civil action under s.1(3) of RIPA). On both a public or private network, the DPA might provide redress for eavesdropping but not if the listener is using a non-digital device or is collecting the information for "personal, household and family affairs". And, again, there will be no actionable harassment unless the interception occurs more than once.

distress after being filmed in the shower by her boyfriend's flatmate, for the claimants in *Hamberger v Eastman* and *Roach v Harper* whose landlords installed listening devices in their homes, nor for the women in *Harkey v Abate* and *Benitez v KFC National Management* who were watched using bathroom facilities.[72] The claimants in *Reklos v Greece*, who brought a successful action in Strasbourg after their baby was photographed without their permission, would also fail in a privacy bid in the United Kingdom.[73] Even the civil claim of the tabloid telephone hacking victims is not straightforward in cases where publication did not result; at the moment, claimants are relying on a broad interpretation of the breach of confidence action.[74] It is clear, then, that neither the right to privacy nor its Article 8 counterpart, the right to respect for private life, is being comprehensively protected in English law. This section will consider how the common law might remedy that shortcoming.

A. Support for Enhanced Physical Privacy Protection

Although the proposition from *Wainwright v Home Office* that there is no general right to privacy in English law still stands, there is considerable judicial support for a conception of privacy which extends beyond the protection of private information.[75] As early as 2001, Mustill L.J. recognised the physical aspects of the privacy interest when he said:

> To my mind the privacy of a human being denotes at the same time the personal "space" in which the individual is free to be itself, and also the carapace, or shell, or umbrella, or whatever other metaphor is preferred, which protects that space from intrusion. An infringement of privacy is an affront to the personality, which is damaged both by the violation and by the demonstration that the personal space is not inviolate.[76]

Similar breadth can be found in some of the judgments in *Campbell v MGN Ltd.*[77] Lord Nicholls held that the misuse of private information action affords respect for just "one aspect of an individual's privacy": "An individual's privacy can be invaded in ways not involving publication of information. Strip searches are an example".[78] Lord Hoffmann also said that the focus of the action had shifted away from "the duty of good faith

[72] *C v Holland* [2012] NZHC 2155, [2012] 3 N.Z.L.R. 672; *Hamberger v Eastman* 206 A.2d 239 (1964); *Roach v Harper* 105 S.E.2d 564 (1958); *Harkey v Abate* 346 N.W.2d 74 (Mich.App. 1983); and *Benitez v KFC National Management* 714 N.E.2d 1002 (Ill.App.2 Dist. 1999).

[73] *Reklos and Davourlis v Greece* (Application no. 1234/05) [2009] E.M.L.R 16 (discussed in "Physical Privacy in Strasbourg" above).

[74] See *Voicemail Claimant v Newsgroup Newspapers and Glenn Mulcaire*, Generic Particulars of Claim.

[75] *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 A.C. 406, at [31]–[32].

[76] *R v Broadcasting Standards Commission, ex parte British Broadcasting Corporation* [2001] QB 885 (CA), at [48]. See also [33] (per Lord Woolf M.R.).

[77] *Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457.

[78] Ibid. at para. [15].

applicable to confidential personal information and trade secrets alike" to the "protection of human autonomy and dignity".[79] The action, he said, now encompasses both "the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people".[80]

Taking this one step further, some courts have suggested, consistently with *Reklos v Greece* and *Söderman v Sweden*, that the taking of a photograph can itself be an actionable breach of privacy.[81] In *Mosley v News Group Newspapers Ltd.*, Eady J. said that, although the pleaded claim was confined to publication of information, "[n]aturally, the very fact of clandestine recording may be regarded as an intrusion and an unacceptable infringement of Article 8 rights".[82] The Court of Appeal in *Murray v Express Newspapers plc* also declined to rule out the possibility that merely taking a photograph of a child in a public place could engage Article 8.[83] Other cases have recognised the negative effects of being watched and followed when imposing liability for publication of intrusive images. For example, the fact that the young boy in *Murray* was expressly targeted by photographers acting surreptitiously bore directly on the Court of Appeal's decision not to strike out his claim for a misuse of private information.[84] And, in *Campbell*, Baroness Hale held that publication of a photograph of the claimant outside a Narcotics Anonymous meeting "added to the potential harm, by making her think that she was being followed or betrayed, and deterring her from going back to the same place again".[85]

The concept of "intrusion" has also been recognised in name suppression cases. In *Goodwin v News Group Newspapers Ltd.*, for example, Tugendhat J. began his discussion of the reasonable expectation of privacy by saying:

> The right to respect for private life embraces more than one concept. [There are] … two core components of the rights to privacy: "unwanted access to private information and unwanted access to

[79] *Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [51].
[80] Ibid.
[81] *Reklos and Davourlis v Greece* (Application no. 1234/05) [2009] E.M.L.R 16 and *Söderman v Sweden* (Application no. 5786/08), Judgment of 12 November 2013, not yet reported (discussed in "Physical Privacy in Strasbourg" above).
[82] *Mosley v News Group Newspapers Ltd.* [2008] EWHC 1777 (QB), [2008] E.M.L.R. 20, at [17]. See also the HRA case of *Wood v Commissioner for Police of the Metropolis* [2009] EWCA Civ 414, [2009] 4 All E.R. 95, at [34] and [36] where Laws L.J. held that although the bare act of taking a photograph on the public street is not capable of engaging Article 8, it could if "aggravating features" such as harassment, hounding, assault, or intrusion into a person's home were present.
[83] *Murray v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch. 481, at [17]–[18].
[84] See *Murray v Express Newspapers plc* [2008] EWCA Civ 446, [2009] Ch. 481, at [54]–[57] and the suggestion by the authors of *Gurry on Breach of Confidence* that "what may have concerned the Court of Appeal most in *Murray* was the *intrusion* into one's private life, rather than disclosure of private information" (Aplin et al., *Gurry on Breach of Confidence*, note 45 above, at [7.97] (original emphasis)).
[85] *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [155]. See also ibid., at [75] (per Lord Hoffmann), [123] (per Lord Hope), but compare [30] per Lord Nicholls.

> [or intrusion into] one's . . . personal space" . . . I shall refer to the two components of the right as "confidentiality" and "intrusion".[86]

He then went on to consider "confidentiality" and "intrusion" separately and, significantly, concluded that although publication of the claimant's mistress's name would not be a breach of her reasonable expectation of "confidentiality", it would be an actionable intrusion.[87] Eady J. took a similar approach in *CBT v News Group Newspapers Ltd.* to the continued suppression of the name of an adulterous footballer who had been identified on social networking sites. He said that "[i]t is important always to remember that the modern law of privacy is not concerned solely with information or 'secrets': it is also concerned importantly with *intrusion*".[88] Both judges used the term "intrusion" to refer to the effects of publication on the individuals concerned and not just to interference with the physical privacy interests which are being discussed here.[89] However, both also expressed concern about the "cruel and destructive media frenzy" likely to engulf the claimants and their families if the injunctions were lifted.[90] Such a frenzy would inevitably have included unwanted surveillance, photography and following. A desire to protect the claimants against such activity was clearly part of the judges' reasoning.

B. Extending Breach of Confidence

The dicta just outlined suggest that there is judicial support for a wider conception of the privacy interest and at least some willingness to extend physical privacy protection in the right circumstances. The next question is how courts might provide such protection where spying, eavesdropping and recording are concerned.

Although the legislature has often recognised the need to protect individuals from eavesdropping, spying and unwanted recording, enactment of a

[86] *Goodwin v MGN Ltd.* [2011] EWHC 1437 (QB), [2011] E.M.L.R. 27, at [85] citing N. Moreham in M. Warby, N. Moreham and I. Christie (eds.), *Tugendhat and Christie's Law of Privacy and the Media*, 2nd ed. (Oxford 2011) at paras. [2.07], [2.08], [2.16] and [12.71]. Tugendhat J. said that the importance of "intrusion" has been recognised by Parliament with the enactment of the PHA and the HRA (*Goodwin*, ibid., at para. [86]). It should be noted, however, that Tugendhat J.'s concept of intrusion differed slightly from that promulgated by this author in the paragraphs which he cited in *Goodwin* (ibid.).

[87] See particularly, *Goodwin v MGN Ltd.* [2011] EWHC 1437 (QB), [2011] E.M.L.R. 27, at [109], [111] and [120].

[88] *CBT v News Group Ltd.* [2011] EWHC 1326 (QB), at [23] (original emphasis).

[89] Eady J. was concerned about the "intrusion", "distress" and "embarrassment" occasioned by "wall-to-wall excoriation in national newspapers" (*CBT v News Group Ltd.* [2011] EWHC 1326 (QB), at [24]). Tugendhat J. emphasised the "distress" which publication was likely to cause and the relationship between "intrusion" and harassment (see *Goodwin v MGN Ltd.* [2011] EWHC 1437 (QB), [2011] E.M.L.R. 27, at [114]–[118]). See also *CBT v News Group Ltd.* [2011] EWHC 1334 (QB), at [3].

[90] See *CBT v News Group Ltd.* [2011] EWHC 1326 (QB), at [24] and [26]; *CBT v News Group Ltd.* [2011] EWHC 1334 (QB), at [3]; and *Goodwin v MGN Ltd.* [2011] EWHC 1437 (QB), [2011] E.M.L.R. 27, at [120]. See also *von Hannover v Germany* (Application no. 59320/00) (2005) 40 E.H.R.R. 1, at [68].

specific physical privacy action seems unlikely. Breach of confidence and misuse of private information could however be developed to provide such protection. Post-*Tchenguiz*, the best argument available to a claimant who has been a victim of telephone hacking, spying, or surreptitious filming, without subsequent or threatened publication, is that he or she has suffered a breach of confidence. As outlined above, the Court of Appeal held in *Tchenguiz* that a person will breach another's confidence if he or she "*looks at* a document to which he has no right of access and which contains information which is confidential to the claimant".[91] In other words, the claimant in that case was able to recover because the defendants had *acquired* private information about him without his consent. As the Court of Appeal said, this is unacceptable because:

> It is of the essence of the claimant's right to confidentiality that he can choose whether, and, if so, to whom and in what circumstances and on what terms, to reveal the information which has the protection of the confidence.[92]

Courts can therefore restrain defendants from looking at the documents again, even if they have no intention of revealing their contents to others: this is because "given that the information is confidential, the defendant should not be seeing it" and "whatever the defendant's intentions, there would be a risk of the information getting out".[93] Further, the Court of Appeal's formulation of the action made it clear that privacy as well as confidentiality was at stake in *Tchenguiz*. Lord Neuberger M.R. held that in cases where Article 8 interests are being considered, "whether the claimant had a 'reasonable expectation of privacy' in respect of the information in issue, is … a good test to apply when considering whether a claim for confidence is well-founded".[94] That test was then applied to determine whether there was a breach of confidence in that case.[95]

It follows that *Tchenguiz* has significant implications for protection against unwanted watching, listening and recording without subsequent publication. If a person can be liable for acquiring private information by looking at or copying confidential documents, then why not also for acquiring private information by other means? More particularly, if it is breach of confidence to obtain private information by reading a document, can it not also be a breach of confidence to obtain private information by watching, listening or recording people; by intercepting their telephone calls, bugging their private conversations or watching them in their homes, for example? The Court of Appeal's reliance on the Strasbourg telephone monitoring

[91] *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [72] (emphasis added).
[92] Ibid., at [69].
[93] Ibid., at [72]. The defendant may change his or her mind or inadvertently reveal the information (ibid.).
[94] Ibid., at [66].
[95] Ibid., at [77].

case of *Copland v United Kingdom* supports this reading of the case. Liability for merely looking at confidential documents is, according to the Court of Appeal in *Tchenguiz*, consistent with the European Court's conclusion that monitoring private telephone calls could be a breach of Article 8.[96] The Court of Appeal therefore clearly thought that *Copland* and *Tchenguiz* were addressing the same issue – the unwanted acquisition of private information – irrespective of differences in the way the information was obtained (the state in *Copland* was tracking telephone usage, not accessing private documents). Support for a broad interpretation of *Tchenguiz* is also found in the observation that the claimant's right to "choose whether . . . to whom and in what circumstances and on what terms, to reveal the information" is the essence of the breach of confidence action.[97] These same choices are undermined when someone obtains confidential information through the use of the senses.

It is suggested then that courts could legitimately decide that it is a breach of confidence to acquire private information through the use of the senses (by hacking a person's telephone calls, bugging a private dinner conversation or videoing an intimate encounter, for example) even if no further use is made of the material.[98] It follows that limited redress for physical privacy breaches can be provided by breach of confidence: as long as confidential information is obtained in the course of the intrusion, liability could be imposed on those who eavesdrop, spy on or record other people even if no dissemination or other misuse of the information results.

Extending breach of confidence would not, however, fill the conceptual gap which has been identified in this article. This is because, in order to establish a breach of confidence, the claimant must be able to point to private information which was obtained as a result of the intrusion. In some cases, this will be unproblematic; if, for example, a telephone hacker hears callers discussing a secret affair, an unannounced miscarriage, or confidential marital difficulties. But in other cases, the information obtained will be anodyne, unimportant or already widely known. The hacker might hear, for example, discussion of celebrity gossip or plans for a holiday which have already been publicised in the media. In these cases, even if the intrusion is serious, the value of the information is low. Further,

[96] Ibid., at [68] citing *Copland v United Kingdom* (Application no. 62617/00) (2007) E.H.R.R. 37. This reasoning also suggests that modern courts would be unlikely to follow Sir Robert Megarry V.C.'s statement in *Malone v Commissioner of Police (No. 2)* [1979] 1 Ch. 344 at 376–77; [1979] 2 All E.R. 620 (Ch.D.) at 645–46 that those who speak on the telephone accept the risk, which he said is inherent in the system, of being inadvertently or deliberately overheard. See also *Malone v United Kingdom* (Application no. 8691/79) (1984) 7 E.H.R.R. 14 in which the applicant's Article 8 claim was upheld.

[97] *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [69].

[98] The telephone hacking claims against Newsgroup Newspapers Ltd have been pleaded, and many settled, on the basis that the defendants have breached the claimants' confidence (and misused their private information) by obtaining and recording their mobile telephone voicemails (see *Voicemail Claimant v Newsgroup Newspapers and Glenn Mulcaire*, Generic Particulars of Claim, especially at para. [25]).

although it is a serious breach of privacy secretly to spy on a person in the shower, to film a child changing at a swimming pool, or to record a father playing with his children in their bedroom, it is unintuitive to say that private "information" is obtained by the intruder. The objection is, instead, to the fact that the voyeur is looking at the claimant when he or she does not wish to be observed; that the watcher has insinuated himself or herself in at a private moment.[99]

Courts could possibly skirt around these difficulties by saying that the intrusive *way* that information is acquired can, without more, make it confidential. In other words, the fact that the information was acquired by eavesdropping or spying could, on its own, be enough to make it confidential. But courts have so far shown little willingness to take this approach. In *Coogan v News Group*, for example, the Court of Appeal held that "[w]here a person's voice messages are intercepted, particularly over a period, there will often be some messages which contain confidential information and some which do not".[100] The fact that the information was obtained by unauthorised telephone hacking was not enough on its own to establish confidentiality.

Alternatively, it might be possible to recharacterise as "information" the subjective impressions one gets when looking at or listening to a person engaged in private activity. For example, the voyeur could be said to get "information" about how the person goes about showering, about what the child looks like naked, and how the father interacts with his children. And the telephone hacker gets information about what the participants were talking about, the exact words used, tone of voice, intimacy or lack thereof. Again, though, there is no evidence that courts would be prepared to interpret "information" in this artificial way and it would be regrettable, even if they were, to place physical privacy protection on such flimsy foundations. It would be too easy on this approach to dismiss as insignificant the amount and quality of the "information" obtained by hackers and voyeurs. What information would be obtained, for example, if the intruder had already seen the child or the woman naked many times before? Further, and more fundamentally, it is artificial to speak of the "information" obtained by unwanted observation. The sensory objection at the heart of these cases – that it is inconsistent with individual dignity and autonomy

[99] See "Theoretical Conceptions of Physical Privacy" above.

[100] *Coogan v News Group Newspapers Ltd.* [2012] EWCA Civ 48, [2012] 2 W.L.R. 848, at [53]. It is also unclear whether the defendants in *Tchenguiz* would have been liable if the computer turned out merely to contain publicly available or otherwise anodyne information. Although the court stressed that the defendant was not required specifically to identify confidential information contained in the computer documents, it did so on the basis that it was obvious that at least some of the documents (many of which related to the claimant's family and private life, his personal and family assets and business dealings) must contain such material (*Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [77]).

to look at, listen to or record a person without leave – is obfuscated if courts are forced to shoehorn them into information-based actions.

So, although it is possible to extend breach of confidence to protect against information obtained by unwanted watching, listening or recording without subsequent dissemination, this will only protect claimants if their objection is to the acquisition of private information and not the act of spying or eavesdropping itself. Whilst there might be situations where this is the case – where the intruder finds out about a previously secret abortion, medical condition, or romantic affair, for example – it will not always be so. As a result, breach of confidence cannot provide principled, coherent protection for physical privacy interests.[101]

C. Extending Misuse of Private Information

The remaining question, then, is whether misuse of private information can be extended to protect physical privacy interests instead of breach of confidence.

It will be recalled that courts considering misuse of private information ask two main questions: whether the claimant had a reasonable expectation of privacy in respect of the information and, if so, whether that privacy interest should yield to the defendant's Article 10 right to freedom of expression.[102] Could courts, in an appropriate case, recognise that a reasonable expectation of privacy is breached by unwanted looking, listening or recording without subsequent dissemination of the material?

It is suggested that they should. As Whata J. said when justifying a similar extension to the New Zealand privacy tort in *C v Holland*:

> a tort of intrusion upon seclusion is entirely compatible with, and a logical adjunct to, the *Hosking* tort of wrongful publication of private facts. They logically attack the same underlying wrong, namely unwanted intrusion into a reasonable expectation of privacy.[103]

So, in both physical and informational privacy cases the fundamental objection is the same: the defendant is obtaining unwanted access to a person by interfering with his or her reasonable expectation of privacy. And both physical and informational privacy breached undermine the claimant's dignity, autonomy and relationships, leading to feelings of distress, mistrust and violation. As Lord Hoffmann has recognised, it is these underlying

[101] The authors of *Gurry on Breach of Confidence* agree and observe that, "if English courts seek to protect against 'intrusions' into private life as well as disclosure of private information then the connection to breach of confidence will become increasingly tenuous, and the case for recognising a separate tort of privacy much stronger" (Aplin et al., *Gurry on Breach of Confidence*, note 45 above, at [7.102]).

[102] See, for example, *McKennitt v Ash* [2006] EWCA Civ 1714, [2008] Q.B. 73, at [11]; and *Campbell v MGN Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [17]–[21] (per Lord Nicholls).

[103] *C v Holland* [2012] NZHC 2155, [2012] 3 N.Z.L.R. 672, at [75]. Raymond Wacks asks, in a similar vein: "If 'privacy' is protected by Article 8 – and [*Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457] bristles with sweeping pronouncements of its significance – why is 'intrusion' excluded?" (Wacks, *Privacy and Media Freedom*, note 10 above, at p. 246).

values of autonomy and dignity which lie at the heart of the misuse of private information action, not "the duty of good faith applicable to confidential personal information and trade secrets alike" which underpinned the breach of confidence interest.[104] It follows that there would be nothing to stop courts from extending the reasonable expectation of privacy test to include situations where the claimant has simply been looked at, listened to, or recorded without leave.

As with the development of misuse of private information, the horizontal effect of Article 8 could provide the impetus for making this change. As discussed above, courts developing "applicable" common law principles – including misuse of private information – are bound to develop the law consistently with the Article 8 right to respect for private life. That right extends well beyond the protection of private information; citizens also have a right to protection from, inter alia, visual and audio surveillance, bodily searches and unwanted photography. The United Kingdom has positive obligations to protect against interference with these interests. It is therefore entirely defensible – indeed, some would say, necessary – for courts to extend the reasonable expectation of privacy to cover these wider private life interests.[105]

If courts are prepared to read it expansively, *Tchenguiz* provides further support for broadening the privacy action to protect physical privacy. As outlined above, in breach of confidence cases involving personal information, courts use the reasonable expectation of privacy test to determine whether confidence has been breached.[106] And, as the Court of Appeal said in *Tchenguiz*, "the law should be developed and applied consistently and coherently in both privacy and 'old fashioned confidence' cases, even if they sometimes may have different features".[107] It follows that if the mere acquisition of private information can interfere with a claimant's reasonable expectations of privacy in breach of confidence, it will also breach the claimant's reasonable expectations in misuse of private information. Reading a person's diary, hacking his or her emails or copying his or her medical records is therefore highly likely to be an actionable breach of privacy. Once courts reach this conclusion, it is – as discussed in the breach of confidence context above – a small step to conclude that it is also a misuse of private information to acquire information by other means; by spying on a person as he or she attends a medical appointment, by bugging a private dinner conversation, or installing a video in his or her home. It is suggested that courts should take this small step and go one

[104] *Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457, at [51].
[105] See the section headed "Physical Privacy in Strasbourg" above.
[106] *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 W.L.R. 592, at [66]. See also "Extending Breach of Confidence" above.
[107] Ibid., at [67]. The court was explaining why it should draw on misuse of private information cases in the breach of confidence context but the converse also applies.

further – they should drop the language of information altogether and recognise that unwanted watching, listening and recording are breaches of privacy in themselves.

Wainwright v Home Office would not prevent courts from doing this. Although Lord Hoffmann was opposed to recognition of a broad-ranging right to privacy, he did contemplate the incremental development of privacy protection.[108] Extension of misuse of private information would be such a development; no general right to privacy would be created. And to the extent that recognition of physical privacy is inconsistent with the specific conclusion reached in *Wainwright* – that there was no right of action available to prison visitors who were strip-searched in contravention of prison rules – things have moved on. Article 8 of Schedule 1 to the HRA would now provide the Wainwrights with a cause of action[109] and Lord Hoffmann's doubts about whether the intrusive strip-search would have breached Article 8 were shown to be ill-founded in Strasbourg.[110] Protection of physical privacy is, then, a logical next step in the development of the right to privacy in private law.

VI. A New Physical Privacy Action

So, when a suitable case arises courts should recognise that it is an actionable breach of privacy deliberately to watch, listen to and/or record a person who has a reasonable expectation of privacy, irrespective of whether "information" is obtained or disseminated. The focus of the action should be on the intrusiveness of unwanted watching, listening and recording itself. The language of "confidence" and "information" should therefore be abandoned in favour of the label "physical privacy".[111] As in misuse of private information, a variety of factors should bear on the existence of a reasonable expectation of privacy: the attributes of the claimant; the nature of the activity in which the claimant was engaged; the place at which the activity occurred; the nature of the intrusion; the absence of consent and whether it was known or could be inferred; and whether the observation was surreptitious or open.[112]

[108] See *Wainwright v Home Office* [2003] UKHL 53; [2004] 2 A.C. 406, at [28]–[33].

[109] Indeed, the HRA had already been enacted when *Wainwright v Home Office* was decided but it did not apply in that case because the strip-search took place in 1997 (see *Wainwright v Home Office* [2003] UKHL 53; [2004] 2 A.C. 406, at [34]).

[110] The European Court of Human Rights held that the guards' conduct breached the claimants' right to respect for private life in Article 8 of the Convention (*Wainwright v United Kingdom* (Application no. 12350/04) (2007) 44 E.H.R.R. 40).

[111] The label "physical privacy" is favoured over "intrusion", first, because unlike "intrusion", "physical privacy" describes what is being protected rather than a particular kind of privacy interference and secondly, because "intrusion" has already had a number of meanings ascribed to it, most of which are broader than the idea of sensory access being described here (see note 12 above).

[112] Liability should not depend on the making of a recording although this would usually be an aggravating feature. This list of factors is loosely based on that set out by the Court of Appeal in the misuse of private information case of *Murray v Big Pictures* [2008] EWCA Civ 446, [2008] 3 W.L.R. 1360, at [36]

The action should not be overly broad. The archetypal case would involve observing or recording an intimate conversation, domestic life, or activities (such as sexual activity, medical procedures, changing, or using a bathroom) during which private body parts are exposed. Since the action is predicated on the need to protect the human values of autonomy and dignity, it should only avail natural persons – corporations, companies and other artificial persons should not be able to rely on it. But the action could potentially be relied on by people who suffer serious physical intrusions in public places: it could, for example, provide redress to those who are closely and deliberately filmed in public whilst their intimate body parts are involuntarily exposed or bugged in public during an otherwise inaudible conversation.[113]

It is important though that the new physical privacy action does not interfere with legitimate attempts to expose harmful or wrongful behaviour or with the appropriate reporting of newsworthy events. Courts should therefore ensure that claimants cannot use the physical privacy action to circumvent the balance between privacy and freedom of expression which has been negotiated in misuse of private information cases. Physical privacy should thus only cover the sensory observation and recording of an individual. Unwanted access to personal digital or paper files – being informational in nature – should remain part of an extended misuse of private information/breach of confidence action. A defence should also be available to a defendant who reasonably believed, at the time that it was undertaken, that the unwanted spying, listening or recording was necessary to expose harmful or wrongful behaviour.[114] As with misuse of private information, the more intrusive the conduct, the more compelling must be the justification for it. It should be almost impossible, for example, to justify the filming of a person using a toilet but relatively easy to justify the surreptitious recording of an otherwise consensual encounter such as a telephone call or face-to-face meeting. Liability for criminal offending would, of course, remain. Finally, where the claimant is recorded in a public place, a defence should

although the last factor is novel and inquiries into the purpose for the intrusion and its effect on the claimant have been omitted since, as Kirsty Hughes has persuasively argued, these factors should "be addressed at the second stage when weighing up competing rights and interests" (K. Hughes, "A Behavioural Understanding of Privacy and its Implications for Privacy Law" (2012) 75 M.L.R. 806, 828).

[113] For further discussion of the kinds of factors which might bear on the existence of a reasonable expectation of privacy in public places, see N. Moreham, "Privacy in Public Places" (2006) 65 C.L.J. 606 and Hughes, note 112 above. The action might also cover those who are filmed or audio-recorded in public whilst experiencing medical trauma, receiving bad news, or experiencing an intimate or traumatic event such as a loved one's funeral or the aftermath of a car accident or crime, (see Moreham, ibid.).

[114] The word "necessary" is intended to imply that the defendant could not have exposed the truth using less intrusive means. For a useful discussion of defences in the American context, see L. Lidsky, "Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It" (1998) 73 Tul. L. Rev. 173. The defence would not, it is suggested, justify wide-ranging state surveillance of citizens of the type revealed by former contractor to the United States National Security Authority, Edward Snowden.

be available if the recording was part of an appropriate attempt to capture a disaster or other newsworthy event.[115]

A physical privacy action, thus formulated, could coexist happily with misuse of private information. In the usual case, liability for breach of physical privacy and misuse of private information would converge. For example, a claimant who had his or her telephone hacked and the contents of the conversation disclosed would succeed in both actions and be compensated accordingly: in the first place, for any feelings of vulnerability, violation and mistrust engendered by the eavesdropping; and then for the embarrassment, violation and possible pecuniary damage caused by the disclosure.[116] A right to watch, listen or record will not, however, always lead to a right to disseminate. Whilst a concerned son might be permitted to install a camera in his mother's home to investigate suspicions that her carers were neglecting her, he might not be entitled to broadcast the footage obtained. As long as the actions are kept analytically distinct though, problems of compatibility, overlap or double-compensation need not arise. Indeed, greater understanding of the values at the heart of the privacy action should, eventually, be fostered.

VII. Conclusion

Significant progress has been made over the past two decades in the protection of privacy in England and Wales. English law now protects against the acquisition and retention of private information, and against the dissemination of private facts, images and recordings. Courts have also recognised that autonomy and dignity are at stake in these cases. Until physical privacy is brought into the mix, however, vital aspects of the privacy interest will remain unprotected. This article suggests that courts are poised to provide that protection. With just a small conceptual shift sideways, the misuse of private information action can be extended to protect against unwanted watching, listening and recording per se. This would bring English law into line with the jurisprudence of the United States and the European Court of Human Rights and with recent developments in Ontario and New Zealand.

As these jurisdictions have recognised, physical privacy is an important, but increasingly fragile, right. It is hoped that when an appropriate case presents itself, English courts will protect it.

[115] It is suggested that this defence would most obviously apply if the appearance of the claimant was incidental to the filming of an event of significant national or international importance such as the aftermath of a bombing or serious train crash. Where recording of intimate or traumatic events is concerned, the defence should be less likely to apply if the event was a tragic but common one (such as a car accident), if the subject or someone with him or her was asking for the filming to stop, if the filming was otherwise clearly exacerbating the subject's distress, or if the filming did not relate to the newsworthy event itself but to the grief of victims or family members suffered afterwards.

[116] For an example of this approach in the American context, see *Schulman v Group W Productions Ltd.* 955 P.2d 469 (Cal. 1998).