
Caolfhionn Gallagher

Abstract
This paper analyses and considers the impact of a landmark decision by the European Court of Human Rights in January 2003 which highlighted the inadequacy of U.K. law in protecting the privacy of individuals captured on closed-circuit television (CCTV) cameras in public places. The domestic and Strasbourg decisions in the Peck case are assessed. Analysis of the subsequent responses of Government, the Courts and the media demonstrates that the lessons of Peck have yet to be learnt, and the Human Rights Act 1998 has failed to ‘bring rights home’ when it comes to Article 8 of the European Convention on Human Rights (ECHR), which guarantees the citizen the right to respect for private life. Privacy in the U.K. is now at best a residual right: what’s left after each of an array of competing concerns have their say.

“This is a free country, Madam. We have a right to share your privacy in a public place.”
Sir Peter Ustinov, Romanoff and Juliet (1956), Act 1

1 Liberty, London. Privacy@Liberty-human-rights.org.uk
2 Cartoon reprinted with the kind permission of the New York Times.
1. CCTV, Human Rights, Fish and Bicycles

The philosopher Vique’s observation that ‘a man without religion is like a fish without a bicycle’ has regrettably been eclipsed by its paraphrase, the now hackneyed slight credited to a range of feminists, ‘a woman needs a man like a fish needs a bicycle’. To some commentators, there is a similar conceptual mismatch between the issue of CCTV and the use of a human rights framework of analysis; for them, CCTV is the fish and rights language the bicycle. The juxtaposition of CCTV and human rights is considered variously as misguided, wrong-headed, overstated or hysterical. David Brin bemoans the “shrill, paranoic rants by conspiracy fetishists who see Big Brother lurking around every corner”; Nikolas Rose is critical of the knee-jerk, unthinking use of terms such as ‘electronic Panopticon’ and ‘society of control’; many criminological and sociological commentators on CCTV issues focus almost exclusively on effectiveness questions and thus, explicitly or implicitly, reject “the occasional complaints of the civil liberties lobby”; CCTV is usually an absentee topic in legal texts on the Human Rights Act 1998 (HRA) generally and the right to privacy in particular.

Underpinning such reluctance to countenance CCTV as a potential human rights issue are a number of factors. Firstly, CCTV is generally installed or used for a stated benign purpose, such as “public safety” or another “sensible-sounding good”. Covert use of video surveillance has been used in high-profile criminal cases to snare child abusers and murderers. The Home

---

3 The phrase was incorrectly attributed to the feminist Gloria Steinem by Time magazine in August 2000, an error Steinem corrected in the following edition’s letters’ page: “in your note on my new and happy marital partnership with David Bale, you credit me with the witticism, ‘a woman needs a man like a fish needs a bicycle.’ In fact, Irina Dunn, a distinguished Australian educator, journalist and politician, coined the phrase back in 1970 when she was a student at the University of Sydney. She paraphrased the philosopher who said, ‘Man needs God like fish needs a bicycle.’ Dunn deserves credit for creating such a popular and durable spoof of the old idea that women need men more than vice versa.”


6 See e.g. Nic Groombridge, ‘Crime Control or Crime Culture TV?’ (2002) 1 Surveillance and Society 30. He initially claims that his paper considers both the ‘pragmatic’ criminological arguments and ‘the civil liberties arguments’, but the only references to the latter in the 16-page article consist of half a paragraph referencing the Privacy International website and a number of ‘refusenik’ comedians, and a separate mention of the ‘function creep’ objection to CCTV. In addition, Groombridge assumes that the ‘pragmatic criminological’ arguments and the ‘civil liberties’ arguments are unrelated and usually at odds - he states that, “it is not easy to encompass the pragmatic criminological effectiveness argument within the principled human rights/civil liberties objections”. In fact, the classic civil libertarian objection to CCTV is that the state should not interfere in the citizen’s life unless it can show a legitimate, effective and proportionate reason for so interfering, a position which incorporates the ‘pragmatic’ within the ‘principled’.

7 Legal journalism and texts dealing with the Data Protection Act 1998 (“DPA”) are exceptions.


9 See e.g. Re D.H. (A Minor) (Child Abuse) [1994] 1 F.L.R. 679, in which covert video surveillance of parents who were suspected of child abuse was permitted and the resulting evidence ruled admissible.

10 The most recent and prolific example of this is the Soham murder trial of November and December 2003. Cf. Allan v. U.K., App. No. 48539/99, decision of the E. Ct. H.R., November 5th 2002, in which the covert audio and video surveillance of the applicant within his cell, the prison visiting area and upon a fellow
Office’s online CCTV Initiative includes a poster for download by the owners of small businesses explaining how CCTV will help them cut crime and increase profits and case studies of CCTV in action. The media frequently echoes this trumpeting, approving style of analysis: from preventing vandalism of fire engines on Teeside to helping police find the killers of a grandfather in Rochdale, the technology is presented as a highly effective tool of both deterrence and detection, with few questions raised about civil liberties implications (or its effectiveness, for that matter). The stated policy purposes behind CCTV tend to be silent on the issue of privacy or other rights. Motorway CCTV, for example, supplies ‘useful information for management purposes’ and ‘the images are not being gathered as part of an attempt to exert general control upon human beings but as a detailed map which can supply answers to elaborate inquiries directed at improving institutional operability.’ Such motivations make the characterisation of the spread of CCTV as ‘Orwellian’, indicative of ‘the death of privacy’, the growth of a ‘maximum security society’ or an ‘electronic Panopticon’ seem outlandish. Indeed, the benign purpose behind CCTV installation is sometimes in itself human rights related and provides safeguards for the vulnerable, as in the case of the installation of cameras in police stations and interview rooms.

The second reason why CCTV tends not to be perceived as a human rights issue is primarily a pragmatic one. Discussing whether CCTV in public places constitutes, in itself, an invasion of privacy or other rights is arguably akin to assessing the merits of shutting the stable door when the horse has long since bolted. Technological change in this area far outstrips the pace of regulation. Inspired by Andrew Kantor (‘there’s no going back, and there’s no hiding the information, so let everyone have it’), David Brin works from the assumption that the ‘rights’ debate is lost and exposure of our secrets is inevitable. He argues that, given this reality, the ideal way forward is not to seek more privacy (in vain), but to accept even less and turn this to our advantage as citizens - he thus neatly sidesteps the argument as to whether that reality is acceptable. His central thesis is that ‘light can shine both ways’ and that the information society is ‘an opportunity in disguise’:

Can we stand living exposed to scrutiny, our secrets laid open, if in return we get flashlights of our own that we can shine on anyone who might do us harm - even the arrogant and the strong?

prisoner and the use of the materials so gained at his trial for murder were unanimously found to violate Arts. 6, 8 and 13 ECHR.

16 Whitty, Murphy and Livingstone, above, p. 314; Rose, above.
17 Brin, The Transparent Society, above, p. 14. A similar conclusion is, albeit hesitatingly, reached by Groombridge (above., n. 8), but for different reasons. He suggests that transparency and democratic, open
As the development and spread of CCTV and related technologies has been evolutionary and piecemeal, it is certainly the case that U.K. lawyers are coming to the debate somewhat late. In contrast, the later and lesser spread of such technology in Canada recently engaged the attentions of retired Supreme Court Justice Gerard La Forest, a scenario which appears ridiculous to a U.K. audience.

Whilst Brin’s ‘inevitability’ argument is primarily a pragmatic one, in privacy theory terms he - unknowingly - has a point. Given the prevalence of the ‘reasonable expectation of privacy’ test, and its avoidance of a normative distinction between public and private, early development and rolling out of potentially privacy-invasive technologies in itself changes the nature of what can reasonably be expected to remain private. If the boundaries are pushed hard enough, they in themselves change; or, if one leaves it too late to find an answer, the nature of the very problem will have changed.

Third, objections to CCTV simpliciter tend to be countered by the claim that, as the cameras operate in public spaces, the citizen waives his rights when he chooses to walk by them. The micro is often converted to the macro, with surveillance in closed, limited societies assumed to operate under identical principles to general society - despite the fact that the basic principles of waiver require true voluntariness.

Fourth, the most obvious right that CCTV appears, at first blush, to engage, the right to privacy, is not a ‘mainstream’ right, and is often seen as applying to one of three groups: (i) the celebrity (reinforced by the ‘jurspruience’ of HRA cases dealing with confidentiality); (ii) the ‘privacy anorak’; (iii) the guilty, those with something to hide (again, apparently reinforced by the fact that CCTV and other visual surveillance has received judicial retention related to Article 6 ECHR, due process rights and the use of covertly obtained video footage of individuals committing crimes and admitting crimes).

The commonplace assumption that CCTV and human rights is a bizarre combination was challenged by a landmark decision of the European Court of Human Rights on January 28th 2003. The U.K. was found to have breached Article 8 of the European Convention on Human Rights (ECHR) when a local council passed CCTV footage of a suicidal man to newspapers and T.V. companies for publication and broadcast. The decision raises many interesting practical and theoretical issues concerning the right to privacy in the U.K. It is a timely reminder that CCTV is still very poorly controlled, and that the introduction of an adequate and consistent regulation system (including appropriate remedies) is long overdue. The decision also challenges the orthodoxy of the traditional notion in Anglo-American jurisprudence that there is a relatively use of CCTV is a good thing in itself, without reliance on the ‘inevitability’ argument of Brin’s. Groombridge posits that “instead of arguing for an insular and isolating privacy, we need a greater intimacy, a slightly grubby organism, not the sterility of the cleansed mall bathed in aseptic light and captured on video. This may require greater transparency… Perhaps I am describing an ‘omnicon’ where all watch, or might potentially, watch all. CCTV would then only be objectionable for being closed and our resistance should be aimed at cameras and systems which are not fully democratic.” Other activists suggest the appropriate manner in which to respond to increased governmental surveillance of citizens is to subject the surveillers to surveillance themselves; see e.g. ‘SF Weekly Columnist Suggests Surveilling John Poindexter at Home,’ http://www.politechbot.com/p-04206.html.
simple dividing line between the public and the private, and instead finds that privacy is a nuanced, context-specific concept, and that certain acts, such as suicide attempts, can be inherently private, regardless of whether they take place on a public street rather than in a private dwelling. Rather, the court views the occurrence of an event in a public place as only one element in the overall assessment of whether there has been an interference with private life, other relevant factors including the use made of the material obtained and the extent to which it was made available to the public. ‘Public’ and ‘private’ are presented as opposite ends of a continuum rather than two simple, watertight categories.

Although the impugned incidents in the Peck case occurred before the promulgation of the HRA, judicial, governmental and media responses to the decision over the past twelve months illustrate that neither it nor the Data Protection Act 1998 (DPA) have adequately addressed the shortfall between the requirements of the ECHR and existing privacy protection in domestic law.

2. Peck v. UK: The Road to Strasbourg

(i) The Facts of the Case
The case centred on Geoff Peck, an Essex man in his forties who had been suffering from severe depression, in part due to his partner’s diagnosis with a terminal illness. On August 20th 1995, at 11.30pm, he walked alone down Brentwood High Street, carrying a kitchen knife, and attempted suicide by slashing his wrists. When he reached a central junction at the end of the High Street he leaned over a railing facing oncoming traffic clutching the knife. He was unaware that a CCTV camera, mounted on the traffic island in front of the junction, filmed his movements.

The CCTV footage later disclosed did not show Peck actually cutting his wrists, but did show him at the junction holding the knife. Brentwood Council’s CCTV monitoring operator had a direct visual and audio link to the police, so that if it was considered an incident warranting police involvement was taking place, the images being captured could be switched through to the police. The sight of a man with a knife understandably prompted the operator to notify police, who quickly arrived at the scene and realised Peck was a danger to no one but himself. They took the knife, gave him medical assistance, and brought him to the police station, where he was detained under the Mental Health Act 1983. His custody record refers to his self-inflicted injury to his wrists on arrival and notes that he was examined and treated by a doctor, after which he was released without charge and taken home by police officers. In the circumstances, they exercised their discretion not to charge him with possession of an offensive weapon in a public place.18

CCTV had, at this point, been operational in Brentwood for over a year. The system was thought to be very successful at reducing crime in the High Street area,19 and so the Council decided to publicise this success by releasing a regular ‘CCTV News’ press bulletin and by co-

---

19 Ibid., per Harrison J. at para. 4.
operating with the media on CCTV-related stories. The first bulletin included two still photographs taken from the CCTV footage of Peck to accompany an article entitled, “Defused – the partnership between CCTV and the police prevents a potentially dangerous situation.” The applicant’s face was not masked in the stills. The article noted that an unnamed individual had been spotted with a knife in his hand, that he was clearly unhappy but not looking for trouble, that the police had been alerted, the individual had been disarmed and brought to the police station where he was questioned and given assistance for his problems. The article included the name of a Council employee in the event that readers wished to obtain copies of the pictures.

This press release began a chain of media articles and t.v. items incorporating Peck’s image. First, two local newspapers used the stills to illustrate articles regarding the benefits of the CCTV system, one of which used the headline “Gotcha.” Anglia Television then obtained footage of the incident involving the applicant for use in a local news programme with an average audience of 350,000, in which, at the Council’s oral request, it masked Peck’s face. The masking, however, was inadequate as Peck’s distinctive hairstyle and moustache rendered him easily recognisable to anyone who knew him.

Peck first became aware that he had been filmed on CCTV and that footage had been released when a neighbour mentioned seeing the Anglia programme to his partner. He took no action at this point, according to the court, because he was still suffering from severe depression.

Four months later a second article appeared in one of the local newspapers which had previously used his image, again accompanied by the same still photograph. The article was entitled “Eyes in the sky triumph” and outlined the benefits of CCTV in the fight against crime. At this time the Council agreed to furnish CCTV footage of, inter alia, the applicant to the producers of ‘Crime Beat’, a series on BBC national television which mimics ‘Cops’-style programmes in the U.S. and has an average audience of 9.2 million. The Council passed the full footage of a number of incidents to the BBC, and then orally imposed a number of conditions, including that no one should be identifiable in the footage and that all faces should be masked. Shortly before the ‘Crime Beat’ episode in question was aired, Peck was told by friends and neighbours that they had seen him in advertising trailers, and he at this point complained to the Council. The Council contacted the producers who apologised for failing to mask his image in the trailers, but confirmed that his image would be masked on the programme itself. The Council accepted this, and the CCTV footage was shown that evening on ‘Crime Beat’. Again, the masking was of dubious effectiveness and many of his friends and family recognised him from the programme.

Following the media coverage of the CCTV footage and stills, the applicant was the subject of jokes, taunts, and abuse from neighbours, the assumption being that he was part of a crime
problem. He found this distressing and humiliating. He disclosed his personal problems to members of his family as he felt it necessary to explain the media coverage. He also made a number of media appearances on BBC radio and television, Channel 4, Channel 5 and local and national newspapers to speak out against the publication of the footage and stills which had occurred. It was at this point that his name and the fact that he had been suicidal when the footage was taken first appeared in the media.

In subsequent months, Geoff Peck complained to the Broadcasting Standards Commission (BSC) about ‘Crime Beat’, the Independent Television Commission (ITC) about Anglia’s broadcast, and the Press Complaints Commission (PCC) about the newspaper articles. He also sought judicial review of the Council’s decision to disclose the CCTV footage of him to the media.

(ii) Conceptual Backdrop: The Right to Privacy

This case raises questions concerning the vexed line between the ‘public’ and the ‘private’. The notion of a right to privacy, despite its almost innovative, modern feel, has an extremely long history, having been recognised and protected, in some form, by regimes as distant as those of Classical Greece,23 the Roman Empire,24 and ancient China. It has long played a fundamental role in language, thought, philosophy, political and religious writings and in biological, sociological and anthropological studies in contexts both older and broader than contemporary discussions of privacy generally acknowledge.25 The philosophical distinction between the public and private spheres is long-standing, and some form of boundary between them has been maintained throughout the history of Western civilisation.26 Thus, the vexed line to be drawn by the right to privacy is the divide between the public and the private, between behaviour which is ‘self-regarding’ and that which is ‘other-regarding,’ as Mill conceptualised it.27 Individuals, and

---

23 The Greek city-state had a clear and strict delineation between the sphere of the polis which was common (koine) to all citizens, and the sphere of the oikos, which was a realm (idia) personal to each individual. See further Jürgen Habermas, The Structural Transformation of the Public Sphere, translated by Thomas Burger and Frederick Lawrence (Cambridge, Ma.: MIT Press, 1962), reprinted in part in Richard C. Turkington, George B. Trubow, and Anita L. Allen (eds.), Privacy: Cases and Materials (Houston, Texas: John Marshall Publishing, 1992), p. 3.
27 John Stuart Mill, On Liberty, reprinted by Bobbs-Merrill (Indianapolis, 1956). Mill’s critics point out that the line between self- and other-regarding conduct is not always easy to draw (much has been written regarding the problem of ‘remote harms,’ for example), but the distinction is nevertheless a useful rule of thumb for limiting state power in a way that advances the cause of individual dignity. See e.g. John Gray, Mill on Liberty: A Defence, Routledge (London, 1996), pp. 48–57.
cultures, have always disagreed about this relationship. Aristotle and Locke famously grappled with it, with differing results; Aristotle considered the private sphere to be out of bounds for government, whereas Locke concluded that the state itself is a necessary means for public protection of certain private ends (although Locke’s views would never have been expressed in the first place, of course, were he unable to publish his work anonymously). The term ‘privacy’, however, still suffers from utter definitional incoherence. Does the word, in a legal sense, refer only to ‘informational privacy’, the control of disclosure over personal information, or is a broader interest at stake? Is privacy a purely negative interest, a “right to be let alone”? Or does it have a more positive side, constituting not only a freedom from but also a freedom to? Is the right to privacy distinguishable from the right to dignity, the right to autonomy and the right to bodily integrity? Is privacy a single, yet multi-faceted right, or a cluster of unrelated interests? Is it a broad catch-all term referring to the “supposed preference of individuals to live their lives and maintain their personalities and affairs free from undue intrusion by, and exposure to, the outside world”? Does it have substantive or merely instrumental value? Is it derivative or stand-alone? Is it a civil/political right or does it also involve questions of economic, cultural and social rights? Is privacy simply the opposite of publicity, or is this a false dichotomy? Does privacy conflict with freedom of expression, or are both concepts subsets of a broader legal right to self-expression? Is privacy a personal interest only, or can a

32 The phrase is Judge Thomas Cooley’s, although often wrongly attributed to Warren and Brandeis who used and popularised it. See Thomas C. Cooley, Law of Torts, 2nd ed. (1888), p. 29. It is also misquoted as the right to be ‘left’ alone on a regular basis in academic articles.
34 See Paul Siegel, Privacy and the First Amendment: The Development and Application (to the Gay Rights Controversy) of an Original Model of Privacy, Ph.D. thesis, Northwestern University, 1982. Siegel sets out to discern to what extent the right to privacy in U.S. constitutional and tort law is properly conceived as a first amendment issue. His model of privacy consists of three categories: (i) control over stimulus input; (ii) control over stimulus output; (iii) control over self-regarding conduct. Given this model, freedom of speech and privacy claims are seen to overlap, and Siegel describes the specific areas of overlap and uniqueness. He then applies the model to gay rights litigation, finding that some cases have a freedom of expression focus, some a privacy focus, and others contain elements of both.
company or other non-human legal entity also enjoy privacy rights? If a personal right, can it only subsist so long as the individual is alive, or does it survive death?  

It is the array of such questions which has led to privacy being described as “the most unruly of all our human rights” by Simon Davies, Director of Privacy International, and “a jungle” by Raymond Wacks, who believes the term ‘privacy’ has come to mean nothing as it is now used with so little precision. Many commentators tend to avoid normative definitions, favouring definitions based upon existing laws. This approach is reminiscent of Lord Wedderburn’s description of the “elephant test” (“an animal too difficult to define but easy to recognise when you see it”) and that of another U.S. judge (with somewhat different priorities, presumably) of obscenity and pornography (“I know it when I see it”). That there is little agreement concerning privacy is, in one sense, unsurprising; this goes with the territory. Lack of agreement concerning the ambit of the ‘right’ or rights to privacy, the appropriate method of protection, and its acceptable limitations is endemic, as, of course, privacy means different things to different people, and is valued differently depending on the person and context. A number of surveys in


38 It is the avoidance of normative definitions which has led Professor Frederick Schauer of the Kennedy School of Government at Harvard to recommend the complete abandonment of the terms “public” and “private”. He argues that the terms have an ascriptive rather than descriptive quality about them. An ascriptive term is one which, in the guise of description, is largely evaluative. For example, a jury verdict of “guilty” not only says that the defendant engaged in certain behaviour, but that it is appropriate for the defendant to be punished for that behaviour. See Frederick Schauer, “Can Public Figures Have Private Lives?” in Ellen Frankel Paul, Fred D. Miller Jr. and Jeffrey Paul (eds.), The Right to Privacy (Cambridge: Cambridge University Press, 2000), pp. 293–309 at p. 293. On ascriptive terms, see H.L.A. Hart, “The Ascription of Responsibility and Rights,” Proceedings of the Aristotelian Society, n.s. 49 (1949), pp. 171–82; Hart, “Definition and Theory in Jurisprudence,” in Hart, Essays in Jurisprudence and Philosophy (Oxford: Clarendon Press, 1977), pp. 26–52. Cf. P.T. Geach, “Ascription,” Philosophical Review 69, no. 2 (April 1960). Acription has also been described as “thick descriptions,” in which the moral evaluation of the conduct is inseparable from the description itself (the classic example is the word “rude”).

39 Lord Wedderburn is credited with this ‘elephant test’ by Iain Ross (Australian Industrial Relations Commission), ‘Re-thinking collective and individual rights at work: a reflection and outlook,’ speech to the ACIRRT Conference, Sydney, July 16th 1999. The test is also referenced in Western Excavating (E.E.C.) Ltd. v. Sharp [1978] QB 761, [1978] ICR 221, per Lawton L.J. (he described the test as showing “that you can often recognise something that you cannot define”). It has regularly been quoted outside court: see e.g. Cabinet Office Strategy Unit, ‘Private Action, Public Benefit: Organisational forms for social enterprise,’ September 2002 (referring to the Social Enterprise London website, “trying to define a social enterprise can be like trying to define an elephant – very difficult and not much point, because you know one when you see one”); Christian von Bar, ‘A Common European Law of Torts,’ paper published by the Centro di studi e ricerche di diritto comparato e straniero (Rome, 1996), p. 8.

40 Jacobellis v. Ohio, 878 U.S. 184 (1964), per Potter Stewart J.
the U.S. have revealed that Americans are more concerned with guarding their financial privacy than details of their sexual history, for example, and the confessional culture either inspired or documented by reality T.V. shows demonstrates a willingness by some individuals to blur the line between their public and private lives.

Regardless of its precise boundaries and definition, the notion of privacy certainly incorporates ‘informational privacy’ (possibly its most famous subset), ‘geographical’ or ‘spatial’ privacy, and ‘decisional privacy’, or privacy qua autonomy in decision-making. Privacy is not exclusively informational privacy (the right to privacy extends far beyond the DPA), nor is it exclusively spatial privacy. To paraphrase the U.S. and Canadian judiciary, the right to privacy “protects people, not places”.

Jean Bethke Elshtain41 and Margaret Mead42 document evidence that privacy is a cross-cultural, cross-species universal, although it is context-specific with differing standards of protection. Attempting to find a normative public/private dividing line is next to impossible. There is, to use Rawls’ memorable phrase, no moral Esperanto when it comes to such a matter. Privacy is a multi-faceted, nuanced concept, and notions of the public and the private shift over time. Spatial privacy provides some useful examples. Now, in broad terms, indoors is considered private, outdoors public. However, in medieval plays prying and eavesdropping often took place indoors, and private, snatched, romantic moments took place outside, in gardens and on balconies. Decisional privacy also illustrates the point, as even the most intimate of matters, sexuality and its expression, now considered to be at the core of the right to privacy by the European Court of Human Rights,43 has regularly been considered of ‘public’ concern by various societies. Societies from the Renaissance to the Enlightenment, for example, invested heavily in the regulation of sexual behaviour, considering non-marital sex of any kind to be a public rather than private affair. As these societies placed extreme emphasis on inheritance, paternity, male honour, and the patriarchal control of female sexuality, any engagement in extra-marital sexual relations had consequences for the marital relationship and, therefore, was of concern to society.44

Despite this conceptual confusion, since the HRA, and arguably for the past half century during our political foot-dragging over incorporation of the ECHR, the appropriate litmus test for testing the adequacy of privacy protection in the U.K. is undoubtedly Article 8. Article 8(1) provides


44 See e.g. William Naphy, Sex Crimes (London: Tempus, 2002), p. 15; R. Howard Bloch, Medieval French Literature and the Law (Berkeley, CA.: University of California Press, 1977), p. 242 (he speaks of Medieval society Medieval society as one in which “adultery, the secret deed par excellence, automatically becomes a matter of public policy”); Kathleen Coyne Kelly, Performing Virginity and Testing Chastity in the Middle Ages (London: Routledge, 2000), particularly p. 8 (“both virginity and paternity are essential to the workings of a feudal society that held the bulk of its wealth in private, aristocratic hands and passed on such wealth from father to son. Biological facts do not always correspond to cultural needs, and therefore biology must be supplemented in some way”)}
that “everyone has the right to respect for his private and family life, his home and his correspondence”, and Article 8(2) sets out the qualifications to this right:

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 imposes primarily negative but also positive obligations on the state. It covers a bewilderingly broad array of personal interests, including the right to a family name, the requirement that the state amend post-operative transsexuals’ birth certificates, if so requested, freedom from sexual orientation discrimination, anonymity, a right not to be identified, whether in court, in cyberspace, or anywhere worldwide; and even an obligation on the part of the state to protect its citizens from pollution.

It has been established repeatedly since 1979 that the correct manner in which to interpret qualified ECHR rights is by setting the borders of the protected right broadly, and then ensuring that exceptions to the right are narrowly construed. Exceptions and limitations must be “necessary in a democratic society”, pursue a pressing social need, and the restrictions must be proportionate to the aim (or aims) pursued. Use of the terms “proportionality” and “necessary” will not suffice; Article 8 requires substance, not form. It must be remembered that the adjective “necessary”, according to the European Court of Human Rights, “is not synonymous with ‘indispensable’, nor has it the flexibility of such expressions as ‘admissible’, ‘ordinary’, ‘useful’, ‘reasonable’, or ‘desirable’, and [it] implies the existence of a ‘pressing social need’”. Further, any proportionality assessment must ideally include, to use the language of the Canadian Charter of Rights and Freedoms jurisprudence, a “least restrictive means” assessment: is there an alternative way to achieve the legitimate aim which interferes less with the citizen’s right to privacy?

48 See Venables v. News Group Newspapers [2001] 2 W.L.R. 56 in which injunctions were granted against the whole world to prevent the publication of confidential information which would or might lead to the identification of two now adult murderers.
Peck: The Judgments

(i) The Broadcasting Standards Commission (BSC)
Peck lodged a complaint with the BSC in relation to the ‘Crime Beat’ programme, alleging an unwarranted infringement of his privacy and that he had received unjust and unfair treatment. The BSC upheld both of his complaints. It was noted that the BBC had already accepted that it had meant to mask the applicant’s image and that this had not been done in the trailer due to an oversight. The BSC also considered the masking during the programme inadequate as the applicant had been recognised by viewers who had not seen the trailer. It was accepted that the BBC had not intended that the applicant would be identifiable, but the effect was more relevant than the intention. Despite the lack of malice, the effect was to reveal to the applicant’s family, friends and neighbours an episode which he did not wish to reveal, and this outcome had been distressing and amounted to an unwarranted infringement of his privacy.

The BSC added that the fact that the applicant later chose to speak publicly about this incident did not alter the infringement established. This was a welcome rejection of the BBC’s version of the ‘asking for it’ argument now frequently heard in celebrity confidentiality cases.

The BBC was directed to broadcast a summary of the adjudication of the BSC with the episode of ‘Crime Beat’ on 12 June 1997 and a summary of the adjudication was also published in the ‘Daily Telegraph’ newspaper on 12 June 1997. The remedy of apology and further publicity (again, to a 9.2 million person BBC audience and a national newspaper readership) was completely inadequate and inappropriate for Geoff Peck’s purposes, and illustrates the difficulty for privacy actions before the BSC. Remedies developed for defamation-style incidents do not transfer well to the realm of privacy, as unfairly damaged reputations may be restored by apologies and public statements, but private information, once publicised, cannot be ‘re-privatised’ and the problem is compounded by further publicity.

(ii) The Independent Television Commission (ITC)
The ITC responded similarly to Peck’s complaint concerning the Anglia TV broadcast. Anglia had already apologised to him and admitted it had breached the privacy requirements of the ITC Code. The ITC agreed, noting in particular the implication of the programme that a man carrying a knife was likely to be intent on a criminal act, and the lack of adequate masking. Given the admission and apology, however, no further action was taken.

(iii) The Press Complaints Commission (PCC)
The PCC not only rejected Peck’s complaints regarding the newspaper articles, it did so without a hearing and merely sent him a letter stating reasons. The PCC considered that, as the events in question took place in a town high street, open to public view, the issue of privacy did not arise and the complaint was rejected outright. This intellectually thin, simplistic response made

51 Sections 2(2) (coverage of events in public) and 5 (scenes of suffering and distress).
53 Ibid., para. 27.
no mention of the time of the incident (11.30pm at night), the fact that the street was deserted, nor the lack of signage to inform the public of the CCTV cameras.

Further, the PCC did not consider that the juxtaposition of the photographs and the articles implied that the applicant had committed a crime and it had been made clear that he was released without charge, the second article indicating that the applicant was ill at the relevant time (again, privacy was not considered to be engaged).

(iv) The Domestic Courts

In addition to lodging complaints against the media outlets that broadcast or published the footage, Peck also sought judicial review of the Council’s disclosure of the CCTV footage, arguing that such disclosure had no basis in law (the Council was, he argued, entitled only to use CCTV images for limited statutory purposes which did not include publicity) or, if lawful, was irrational. The substantive application was rejected by the High Court in November 1997. The Court found that the purpose of section 163, Criminal Justice and Public Order Act 1994, was to empower a local authority to provide CCTV equipment in order to promote the prevention of crime or the welfare of victims of crime:

By publicising information about the successful operation of the CCTV, the Council was providing information about its effectiveness and thereby reinforcing the deterrent effect of its operation. The making available to the media of footage from the CCTV film to show the effectiveness of the system can properly be said ... to be incidental to and to facilitate the discharge of the Council’s function under Section 163 because it thereby increased, or tended to increase, the preventative effect of the equipment which [the Council was] providing for the purposes of the prevention of crime.

Publicising the effectiveness of the CCTV scheme was, therefore, incidental to the discharge of the function set out in s. 163, and was therefore within the scope of s. 111, Local Government Act 1972.

As to irrationality, Peck submitted that the Council had acted irrationally in disclosing the footage with the aim of crime prevention when he not, in fact, been engaged in any criminal activity; and that the failure to prevent disclosure of his identity facilitated an unwarranted invasion of his privacy. Harrison J. had some sympathy with that submission, but did not consider it correct in law:

I have some sympathy with the applicant who has suffered an invasion of his privacy, as is borne out by the findings of the Independent Television Commission and the Broadcasting Standards Commission. However, if I am right in deciding that the Council does have power to distribute the film footage.

---

54 It is interesting to note that the case was considered so unremarkable that it was not reported in the All E.R. or the W.L.R.
from its CCTV system, there may on occasion be undesirable invasions of privacy. Unless and until there is a general right of privacy recognised by English law (and the indications are that there may soon be so by incorporation of the European Convention on Human Rights into our law), reliance must be placed on effective guidance being issued by Codes of practice or otherwise, in order to try and avoid such undesirable invasions of a person’s privacy.

The evidence is that the CCTV cameras in public places play an important role in both crime prevention and crime detection. In this case, the film footage showed a man walking in the High Street carrying a large knife in his hand. It did not show him attempting to commit suicide. It was plainly a potentially dangerous situation... It was not unreasonable for the Council to conclude that the footage was a useful example of how a potentially dangerous situation can be avoided.... In those circumstances, it seems to me that the decision of the Council to distribute the film footage to the media could not be said to be irrational or unreasonable.56

The judicial review approach, assuming the behaviour of the Council to be acceptable unless ‘irrational’ or ‘unreasonable’, is diametrically opposed to the appropriate approach to privacy issues under the ECHR. The Convention requires that presumptive weight be given to the right, and the limitations be strictly construed, yet judicial reviews turns this process on its head. The High Court judge found against Peck on the basis that “the Council cannot be said to have acted irrationally in the sense that they had taken leave of their senses or had acted in a manner in which no reasonable local authority could sensibly have acted.”57

Harrison J. also laid weight on the fact that the Council “did not sell the take-outs from the CCTV footage for commercial gain,”58 presumably on the basis that, had payment been given, this would demonstrate mala fides and possibly undermine their justification for the distribution of the footage. He viewed the chain of events as “unfortunate” and recommended that, “with the benefit of hindsight”, the Council consider “tighten[ing] up their guidelines to avoid a similar incident in the future.”59

An application for leave to appeal to the Court of Appeal was rejected, and the subsequent leave application to the Court of Appeal was, again, rejected.60

56 Set out in Peck v. U.K., above, paras. 31, 32.
57 Ibid., para. 32.
58 Ibid., para. 32.
59 Ibid., para. 32.
60 January 21st 1998. The reason given was that, “the [High Court] Judge was plainly correct in his interpretation of the relevant statutory provisions and the Council was neither acting outside its statutory authority nor irrationally in making the film and photographs available to the media. The injury, of which complaint is made, arises from a failure on the part of the media to sufficiently disguise the applicant when making the film and photographs visible to the public. That is and has been the subject of complaint against the media involved but is not capable of supporting a claim for a declaration against Brentwood Borough Council.”
(v) The European Court of Human Rights (ECHR)
Peck applied to the European Court of Human Rights invoking both Article 8 and 13 (the right to an effective remedy). The Court unanimously found breaches of both Articles.

Article 8
In line with the Commission’s decision in *Herbecq v. Belgium*, the Court accepted that “the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual’s private life”. However, the situation may be different where a record is maintained (as in *Amann v. Switzerland*62 and *Rotaru v. Romania*63) or, as in the present case, disclosed. The Court noted that Peck was filmed in a public street, but that he was not there for the “purposes of participating in any public event”, nor was he “a public figure”. The fact that “the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation… and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995”65 gave rise to a “serious interference” with his Article 8 rights.66

The Court then moved to its Article 8(2) analysis. It considered that the disclosure pursued legitimate aims (public safety, prevention of disorder or crime, protection of the rights of others) and that disclosure was permitted by statute as incidental to the Council’s functions. However, as the case did not concern disclosure of footage of the commission of a crime, the question of necessity was vital and particular care was required of the Council. Whilst the strong interest in the prevention of crime and the important role CCTV can play in this regard (a role reinforced by public awareness of its operation) was noted by the Court, it considered that the Council had failed to take adequate steps to protect Mr. Peck’s interests. A range of ‘less restrictive means’ of achieving its objectives without unjustifiably interfering with his right to privacy were listed:

- The Council could have taken steps to identify Mr. Peck via the police and sought his consent;67
- It could have taken steps to mask his identity before passing the footage to the media;
- It could have taken proper care to ensure that the media masked his identity, such as by demanding written undertakings.

Article 13 with Article 8

---

65 Ibid., para. 62.
66 Ibid., para. 63.
67 The Court did note that in certain cases this would be impossible, but in the present case the applicant could easily have been traced and asked for his consent.
The Court examined three options which had been open to Mr. Peck: judicial review; complaints to the media commissions; a breach of confidence action.

Judicial review was, unsurprisingly, considered inadequate for the purposes of providing Mr. Peck with a remedy for a breach of his Article 8 rights. The ‘irrationality’ test applied by the domestic courts could not equate to the required ‘necessity’ and ‘proportionality’ tests. The absence of a legal power to award damages or to restrain publication was considered by the Court fatal to the argument that the media commissions could provide an effective remedy. Finally, the Court found that Mr. Peck would not have had a remedy in breach of confidence, as he would have been unable to establish that the footage had the “necessary quality of confidence” or that it was “imparted in circumstances importing an obligation of confidence”. Further, the Catch-22 resulting from the combination of the fact that he was unaware that the material was being disseminated until informed by others, and the fact that he could not bring an action in respect of material already in the public domain stymied actionability of any of the publications.

The Court awarded substantial costs and EUR 11,800 for non-pecuniary loss to Mr. Peck.

**Peck: The Aftermath**

Despite the - undoubtedly correct - decision on the particular facts, and the useful clarification and elaboration of certain Article 8 principles, the Peck case does raise some unsettling questions which are beyond the scope of this paper. The two most notable questions are, first, how wide does dissemination have to be for the Peck principle to apply? The Court’s emphasis on the sheer scale of the audience numbers, and its reference to how they went beyond what Mr. Peck “could possibly have foreseen,” links uncomfortably to the often inadequate ‘reasonable expectation of privacy test’. The ‘strength of numbers’ approach also undermines a key factor in Peck’s decision to litigate: being recognised by his local community. Of the 9.2 million viewers who watched ‘Crime Beat’, he was most concerned about the small few closest to him. Second, is the Court’s reiteration of the Herbecq principle, that the monitoring of an individual in a public place by a CCTV camera or other remote means does not engage Article 8, sustainable? The Court has posited that monitoring of a public scene by technological means is comparable to someone being observed on the street by someone else in the same location. This ignores the inequality and lack of reciprocity inherent in remote observation.

Nevertheless, the judgment is useful in many respects. It reinforces the fact that Article 8 is not merely a spatial privacy right, applicable to actions which take place in ‘private’ but not in ‘public’ spaces. A key principle of Article 8 jurisprudence has long been that a person’s location is not determinative of the public or private nature of their behaviour and expectations.

---

69 The ITC’s power to impose a fine did not amount to an award of damages.
70 Peck v. U.K., above, para. 62.
Peck establishes that, notwithstanding that a person is in a public place, there can be an interference with his Article 8 rights where a record is created of their actions and the record is disseminated with the result that their actions are communicated to a greater number of people than the person could possibly have foreseen. As James Welch notes, “if it is assumed that the principle extends to other forms of record - photographs or written accounts - it is hard to see how the judgment cannot ultimately lead domestically to some form of privacy law.”

A year on, however, the state of U.K. privacy law is still “as unsettled… as a haystack in a hurricane”. Even the most basic of lessons from the Peck judgment have not been taken on board, by the police, the media, the Home Office, the judiciary or government. Tarrant on CCTV continues to broadcast footage of identifiable individuals captured on CCTV in compromising positions; the media commissions’ remedies remain unaltered; the Information Commissioner’s Guidelines on CCTV remain unchanged since July 2000, and echo many of the unenforced requirements in the Brentwood Borough Council Guidelines of 1994. The Home Office CCTV website now includes a disingenuous summary of the Peck decision, which claims the issues raised are irrelevant given the HRA and restructures the order of the findings so that they read in an overly favourable manner to the Council (for example, it is proudly noted that the Council’s behaviour was found to be “in accordance with law,” a technicality which simply confirms that the conduct had “some basis in domestic law” and was not entirely arbitrary). The same webpage, hilariously, lists a ‘Knowledgebase’ of topics, including CCTV; if CCTV is selected, a list of subtopics appear, including ‘Good Practice’; if this is selected, the response is: “AltaVista Found No Results for Good Practice”.

A briefing newsletter issued by Centrex, the Central Police Training and Development Authority, to all police nationwide has dealt with privacy a number of times over the past twelve months. The guidance given is dangerously misleading and ignores key aspects of the Strasbourg decision in Peck. In July 2003, for example, a page of the Centrex newsletter was devoted to the topic ‘Privacy and Public Places’. The opening sentence baldly states:

The protection of a person’s private life is specific to those acts conducted in private. Where actions are conducted in public the relevant provisions of the Human Rights Act 1998 will not apply.

Again, in October 2003 Centrex advised all police, under the heading ‘Strip-Searches, Right to Privacy and Damages’ that “there is no remedy for damages for an invasion of privacy.”

---

74 See in particular the sections dealing with ‘Privacy to Neighbouring Properties,’ which are identical.
77 Ibid.
78 Centrex Digest, July 2003, p. 49.
79 Centrex Digest, October 2003, p. 34.
One possible, although extremely limited, exception was noted: “damages may be available if intent to cause humiliation and distress through unjustifiable actions can be established.” It was noted that an intention to cause humiliation and distress alone would be insufficient to ground an action; rather, a plaintiff would also have to demonstrate that the actions in question were “unjustifiable.” This two-pronged requirement was based upon an interpretation of the House of Lords’ decision in the unusual and distressing case of Wainwright v. Home Office - another privacy case based on a pre-HRA incident, although it appears in the Centrex Digest pages without such a caveat.

These briefings inform police officers that (i) Article 8 of the ECHR, the right to private life, only applies to acts conducted in private places and (ii) in any event, damages are not generally available for a breach of privacy; both pieces of advice fly in the face of the Peck decision. They return to the simplistic notion of privacy as a spatial issue only, related to place rather than activity or context, and proclaim “the right to share your privacy in a public place.”

In an Employment Appeals Tribunal case in June, this approach was taken, and sexual activity which took place in a café toilet was considered outside the scope of Article 8. Article 8 only protects and covers those acts which are private, and conduct which takes place in a location to which the public have ready access cannot be private, it was held. The small matter of a Strasbourg decision deciding precisely the opposite was ignored; the Tribunal was unwilling to experience what Herbert Spencer once called The Tragedy of the Murder of a Beautiful Theory by a Gang of Brutal Facts.

Government does not appear to have learnt the core lessons of Peck, either. First, the pattern of argument on privacy matters continues (based on the mistaken language of ‘balancing’ and a failure to appreciate how Article 8 should be correctly interpreted). Second, the unsatisfactory process of technological roll-out (technology first, regulatory questions later) continues.

‘Balancing’ Language
The standard rhetoric employed in support of incursions upon citizens’ privacy invariably relates to the need to ‘balance’ the right to privacy against other legitimate governmental concerns, such as the prevention or detection of crime, terrorism, or fraud. However, in the weighting process, privacy almost invariably loses out.

The assumption is that the individual right to privacy is outweighed by the general, collective ‘right’ to national security, crime detection, crime prevention, or whatever other supposed benefit is said to result from a surveillance scheme of wide, or even universal, applicability.

---

80 Ibid.
81 16th October 2003.
82 Above, n. 1.
84 This viewpoint has been advanced by a number of communitarian commentators, the most prolific of whom is Amitai Etzioni. See his The Limits of Privacy (New York: Basic Books, 2000), and, more generally, The Spirit of Community: Rights, Responsibilities, and the Communitarian Agenda (London: Fontana Press, 1995), The New Golden Rule: Community and Morality in a Democratic Society (New York: Basic
This one-size-fits-all-surveillance-methods logic is now being applied to topics such as I.D. cards or communications data. A cost-benefit analysis is conducted, which proceeds on the assumption that privacy is a right of the ‘individual’, whereas convenience, immigration control, terrorist detection and prevention, and the fight against crime are ‘public’ rights; when the debate is set up in this manner, it is inevitable that the individual right is trumped by the collective, public right, the one loses out to the many.

This approach suffers from many flaws: it fails to recognise that ‘individual’ rights are of public and general concern; it ignores the value of privacy as a social and collective value; it also, in suggesting that lone voices should be ignored if the majority of the public agree with ceding aspects of their privacy for what they perceive as the ‘common good’, treads dangerously close to majoritarianism and populism in law-making, an unacceptable approach to human rights’ issues.

This political approach to the contest between privacy and competing rights is also echoed in the Courts. Post-HRA, ‘balancing test’ language has been used in a misleading manner which ignores the correct approach to rights set out in the ECHR. When the ECHR sets out a right, and then sets out a series of possible limitations to that right, the correct approach (as explained by the European Court of Human Rights itself) is not to ‘balance’ the right and the limitations, nor to allow great leeway to the decision-maker to decide how that balancing process operates. Rather, the correct test to use is to give presumptive weight to the right, and then construe the limitations to that right in a narrow manner. Setting the analytical scales up in the manner described above, one versus the many, the individual right to privacy versus the collective right to safety and security, is thus absolutely incorrect.

There are many reasons for the neglect of the correct ECHR approach to privacy questions. One relates to judicial reluctance to abandon or appropriately amend traditional judicial review rules post-HRA. Another relates to the misinterpretation and misapplication in U.K. courts and by U.K. politicians of phrases (such as ‘proportionality’) used in a very specific context in the European Court at Strasbourg. However, arguably the major reason for this neglect relates to the fact that the mainstream debate on privacy in the U.K. has tended to focus on the interplay


86 For powerful arguments on this point see Priscilla Regan, Legislating Privacy: Technology, Social Values and Public Policy, University of North Carolina Press (Chapel Hill, NC, 1995), Chapter 8, and Colin J. Bennett and Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Aldershot: Ashgate, 2003), Chapter 2. Regan sets out a strong argument regarding privacy as a social and collective value, and Bennett and Raab use her work as a springboard for a nuanced argument concerning privacy and equality.


between privacy and freedom of expression, rather than on other aspects of privacy and other competing concerns. Most popular writing on privacy has concerned the paradigm of the sunbathing celebrity snapped by a paparazzo while topless, and, indeed, most recent academic legal writing has been pinned on the conflict between Articles 8 and 10 ECHR, the rights to private life and freedom of expression. Assessing the relative merits of two rights with equal protection under the ECHR, such as Articles 8 and 10, is an extremely different task to the assessment of a right and appropriate limitations to that right, such as Article 8(1) and Article 8(2); when assessing two competing rights, a ‘balancing test’ is appropriate, because of course the right of the individual to privacy (Article 8), the right of the journalist and editor to publish (Article 10) and the right of the audience to be informed (Article 10) cannot all be given presumptive weight. Ronald Dworkin recognises this in his landmark work, Taking Rights Seriously. He argues that ‘balancing’ is only appropriate where two fundamental individual rights clash, and should never be used to weigh a right against competing policy concerns and values; thus, a very different approach is required when Articles 8 and 10 compete to that required when Article 8(1) and 8(2) compete.

The predominant current ‘balancing test’ approach, in which the individual right to privacy is always trumped by a ‘collective’ concern, runs the risk of privacy becoming a residual right only, what’s left after each of an array of competing concerns have their say. This risk is multiplied by the piecemeal approach to privacy issues; in each individual instance, it is accepted that privacy is ‘outweighed’ by a competing concern, and the extent of the right is thus nibbled away, little by little. This process has been described by the commentator Charles J. Sykes:

The truth is that much as we deplore the erosion of privacy – and we can be quite eloquent on the subject – many of us accept the violation in the name of a wide range of equally attractive virtues and interests. To paraphrase Jane Austen, privacy is a value that everyone speaks well of, but no-one remembers to do anything about. No-one disparages privacy to its face. They simply choose to emphasise the public’s right to know, national security, personal safety, conveniences, economic opportunity, politics, ideology, or the pursuit of virtue.

There is an intellectual poverty in the ‘balancing test’ itself, even when privacy is viewed as a purely individual right. However, a number of experts raise another problem with the language of balancing: it fails to recognise that privacy is itself a collective value (in addition to an individual value). Charles D. Raab and Colin J. Bennett, for example, note that the prevailing privacy paradigm is solely individualist, and they argue that this sidelines discussion of privacy protection as a matter of social policy. Similarly, Jack Hirshleifer and Ferdinand

---

Schoeman\textsuperscript{94} claim that privacy is far more than a tool for protecting the individual, but is an organising principle of civil society.

When privacy is viewed in a purely individualist manner, and it is then faced with a ‘collective’ right, such as national security or personal safety, the rationale for overriding the former is often stated to be that if one has ‘nothing to hide, there is nothing to fear’. One U.S. commentator describes this pervasive rationale as follows:

For decades, people have warned that pervasive databanks and surveillance technology are leading inevitably to the death of privacy and democracy. But these days, many people who hear the word ‘privacy’ think about those kooks living off in the woods with their shotguns: these folks get their mail at post office boxes registered under assumed names, grow their own food, use cash to buy what they can’t grow for themselves, and constantly worry about being attacked by the federal government – or by space aliens. If you are not one of those people, you may well ask, ‘Why should I worry about my privacy? I have nothing to hide.’\textsuperscript{95}

This echoes an anecdote told by E.L. Godkin, an early privacy advocate. He told the story of a traveller in a U.S. mining town who pinned a shirt across his open window on the piazza while performing his ablutions; after a few minutes he saw it drawn roughly aside by hand from without, and, when he asked why, a voice answered, “We want to know what it is there is so darned private going on in there?”\textsuperscript{96} The question is still asked and still makes us flinch. Policy questions are regularly posed by government in these terms, assuming that the citizen who resents the retention, inspection or tracking of his personal information is behaving suspiciously. The assumption is that law-abiding citizens have nothing to fear from increased security, the CCTV camera on the street, the I.D. card. This links to traditional religious notions\textsuperscript{97} and, more recently, to feminist jurisprudential ideas\textsuperscript{98} regarding the link between privacy and shame, privacy and wrong-doing. A similar point was also made in 1975 by Dr. Marshall. He referred to the famous ‘definition’ of privacy as “the right to be let alone”\textsuperscript{99} and asked what precisely this
'right’ means: “to go on battering the baby, or cheating the Inland Revenue, or poisoning the customers?” 100 Only the guilty have something to hide, runs the theory.

This rationale is utterly flawed. The ordinary, decent, law-abiding citizen does indeed have much to fear from privacy invasion, not because he or she has done or intends to do anything wrong, but because the State should assume that all individuals have nothing to hide unless it has a specific, compelling, legitimate reason to believe otherwise. The ‘nothing to hide, nothing to fear’ rationale undermines the citizen’s right to be let alone unless the State can demonstrate a compelling reason for interfering, surveying, monitoring, and a method which is proportionate to that aim. Blanket, mass surveillance policies on their face belie any claim to proportionality, and can only be justified if there are compelling arguments in their favour. Further, an examination of the philosophical basis of the right to privacy reveals that every individual does indeed legitimately have something to hide. When someone reads a book over your shoulder on a bus, you will likely feel irritated, not because you are reading something smutty, but because your private space and choices are being intruded upon; equally, most homes have net curtains in the living rooms which conceal nothing more racy than dinner-eating and t.v.-watching, but again, they signify the distinction between private and public space.

Technology First, Questions Later
The lack of intellectually rigorous assessment of ‘light-touch’, generalised privacy issues is exacerbated when discussion of the merits or otherwise of a particular technology are delayed. Given the pace of technological change, and the residual concept of liberty in the U.K. (everything is permitted which is not, expressly or impliedly, forbidden), this results in a technology developing, taking hold, and the postponement of questions. The proliferation of CCTV is an example of this order of events, as is the burgeoning national DNA database. The Regulation of Investigatory Powers Act 2000 (RIPA) also followed this pattern: it was introduced to provide a statutory framework for well-established surveillance activities that had been hitherto unregulated. Similarly, S.I.s introduced in September 2003 (under RIPA) followed this pattern, their explanatory memorandums claiming they were needed to “regulate the unregulated” and “provide ECHR cover for existing activities”.

Essentially, technologies and techniques are being tested in the way an undergraduate supposedly tests spaghetti boiling in a pot of water to see if it is done: throw it against the wall and see if it sticks. In the context of privacy, and the ‘reasonable expectation of privacy’ test now - apparently - favoured even by Strasbourg, this lack of peer review and legal assessment at an earlier point is worrying. The reasonable expectation test is not normative: if you push the limit far enough, the limit itself shifts. We do not only need to assess what type of regulation system is needed for CCTV and other technologies; we must remember that the process, the chain of events itself (technological development, rolling out, and finally, regulation) means that questions about privacy “are changing before our eyes.” 101 The evolving landscape has the

capacity, “if not to end privacy, then to redefine what we mean by the term”. Over a decade ago, one writer set out a simple requirement for a privacy law. In the aftermath of Peck, and the continuing unquestioning advancement of technologies which may impact upon privacy, it is clear that his wish has not yet been granted, “A law of privacy, to be worth anything, ought to have one essential and simple characteristic: it ought to work.”