The Public Private Boundary on the Internet

ICF Legal Subgroup

September 2005

The Public Private Boundary on the Internet

Introduction

1. It is a well-established doctrine that "what is illegal offline is illegal online". A small amount of specialist legislation has proved necessary, and remarkably few legal problems have arisen in prosecuting wrongdoing within this new milieu. Nevertheless, there are significant differences between the online and offline worlds and familiar doctrines may need to be adapted or rethought from first principles. This paper addresses some particular issues that arise within one rather broad area - the distinction that Parliament and the European Court of Human Rights (EctHR) have made between public and private spaces, and the constraints and obligations that follow.

2. What may or may not be a public space is a far from simple question, even in the offline world. Activities that are lawful in a back garden may amount to an offence if performed in the front garden, yet for the house across the street the opposite might be the case. On the Internet, there is a lack of familiar concepts such as hedges, fencing, or people passing by on a public footpath; it is thus even harder to formulate straightforward rules to express the essence of the difference between public and private. Fortunately, the law is robust enough to deal with these difficulties where the matter comes before a court. Whether a particular place is public or private – and hence which laws will be applicable – is a matter of fact that will be for a jury to decide, as has recently been re-asserted by the Court of Appeal[1].

3. For users of the Internet with a need to understand where the boundary between public and private may be found, we find there are no clear legal authorities in respect of the Internet, and so we must proceed by analogy. This paper does not attempt to address the generality of the question as to which parts of the Internet may be public or private. It examines the notion of privacy as it has been developing in the courts and examines how these developing ideas are related to the restrictions placed on law enforcement officers by the Regulation of Investigatory Powers Act when they enter "public" or perhaps "private" spaces on the Internet. Finally, it looks at some specific legislation, such as the law restricting "ticket touts", where activities are forbidden in "public", and asks whether prosecutions for similar activity on the Internet are likely to produce the expected results.

4. Recent cases on privacy have arisen from the never-ending search by celebrities to find respite from the prying lenses of journalists, and have posed the question of how much privacy can be expected in a public place. For those of us who live in a democratic society but have not yet achieved celebrity status, the intrusion of journalists is secondary to our concern that the State does not overstep the mark in its governance and protection of its citizens. At the same time, we have increasingly come to realise that our privacy, in its widest sense, is more likely to be breached by the activities of marketing organisations, and other commercial entities, and, more recently, criminals from organised groups, all of whom have recognised the sterling value of personal data. In life, the boundary between what is public and what is private is far from clear. On the Internet, the boundary is no clearer, and the threat to our privacy is no less real. Any exploration of the public / private divide soon reveals that it is a boundary built upon the elastic concepts of

[1] *R v Hanrahan* (Justice of the Peace, v168, 4 Dec 2004, p947).

expectation and perspective. Despite the uncertainty of the boundary, we know that the activities of hackers, the interception of communications, intrusive surveillance and the use of undercover agents all sit well inside the private area, and so these issues will not be addressed here. What this paper explores is uncertain ground on the frontier of privacy.

What is privacy?

5. Let us begin by reviewing how privacy has been defined. Article 8 of the European Convention on Human Rights states that:

> *Everyone has the right to respect for his private and family life, his home and his correspondence.*

In *PG & JH v UK*[2] the ECtHR recognised that the term 'private life' was not susceptible to exhaustive definition, but noted that gender identification, name, sexual orientation and sexual life had already been found by the Court to be aspects of a "personal sphere" protected by the Convention. In the earlier case of *Niemietz v Germany*[3] the Court thought that sphere was wide:

> *It would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature…*

Summarising this in *PG & JH (at para 56)* the Court said:

> *There is…a zone of interaction of a person with others,* ***even in a public context****,* (author's emphasis) *which may fall within the scope of private life.*

6. In the Regulation of Investigatory Powers Act 2000 (RIPA) – which was introduced to provide a statutory framework for surveillance following criticism of the UK's position by the ECtHR in an Article 8 case[4] – 'private information' in relation to a person is said to include any information relating to his private or family life.[5]

7. The rather wide definition of personal data in the Data Protection Act 1998 – data which relate to a living individual who can be identified – has recently been restricted by the Court of Appeal in the context of data access rights.[6] The mere mention of a data subject in a document does not make it personal data, but private information in another party's possession is subject to the principles set out in Schedule 1 of the Data Protection Act 1998. The processing (which includes collection) of data must be fair and lawful, and in accordance with one of the qualifying preconditions given in Schedule 2. For our purposes, we should note that Schedule 2 purposes include where it is necessary for the administration of justice, for the exercise of any function of the Crown, or "any other function of a public nature exercised in the public interest by any person."

---

[2] *PG and JH v The United Kingdom*, no.44787/98, ECHR 2001-IX
[3] *Niemietz v Germany* (1992) 16 EHRR 97
4 See *Khan v The United Kingdom*, no. 35394 ECHR
5 RIPA 2000, s.26(10)
6 *Durant v Financial Services Authority* [2003] EWCA Civ 1746

8. An alternative qualifying precondition for data gathering is the consent of the data subject, and perhaps the definitions of privacy above should be qualified by the phrase "…the details of which the subject wishes to keep private." In public places, we are surrounded by those who are careless as to their privacy, or by those from whom consent to access their private information may be implied by their actions. The recent idea of blogging – maintaining an online personal diary – is an example of this. On the train, we often have no choice in overhearing other peoples' telephone conversations. They would not receive much sympathy if they complained of a breach of privacy. In the Douglas's case against Hello magazine, in the Court of Appeal[7], Keene LJ thought the celebrities had diminished their claim of breached privacy because they had already sold it to a rival magazine. Privacy may exist in a public place, but the concept is limited by practicality and commonsense, within the compass of reasonable expectation. In the USA, in *Katz v US*[8] the test of this was thought to be

> *..a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and second, that the expectation be one that society is prepared to recognise as 'reasonable'. Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the plain view of outsiders are not protected because no intention to keep them to himself has been exhibited.*

There is no comparable position in English law. The closest to this position is found in the Naomi Campbell case in the House of Lords[9] where Lord Hope approved the finding in *A v B Ltd*[10] that a suit for breach of confidentiality must be underpinned by a desire to keep the subject matter private. But different factors apply when the State is involved. A public authority is subject to the mandatory requirement within Article 8(2), and also to a moral imperative not to be an Orwellian institution, inappropriate in a democratic society. Acting on information accidentally overheard from a careless conversation is one thing; gathering information "accidentally on purpose" is another.

<u>What is public?</u>

9. In *DPP v Greenwood,*[11] Bingham LCJ made a succinct summary. There were numerous authorities to show that private property can be a public place, and the principle to be drawn was that a public place is a place to which the public have access. He continued:

> *The next question that arises is to identify what is meant by the public. The public are those who require no special qualification or membership in order to gain that access. If they have access by virtue of some special qualification rather than as a member of the public, they will not gain access as members of the public and the place to which they gain access will not be a public place…*
>
> *What is the proper approach for distinguishing members of the public from those who have some special characteristic by means of which they gain access? The distinction which has been adopted by this court in the past is to*

7 *Douglas v Hello* [2001] 2 All ER 289
8 *Katz v United States of America* 1967, 389 US 347
9 *Campbell v MGN* [2004] UKHL 22 at para 92
10 [2003] QB 195
11 [1997] EWHC Admin 129

consider whether those gaining access to the area in question have some special characteristic or reason personal to themselves which is not possessed by the public at large. But even if the reason is personal, it may be so common and ordinary that it is not capable of removing those persons who have that personal reason for visiting the area from the category of members of the public.

This seems very pertinent in respect of Internet chatrooms and other fora. A US court has found that chat rooms that will only accept one side of an argument, and which lock out those who disagree, are still public fora, nevertheless[12]. We shall return to chatrooms later.

Is there a boundary?

10. Identifying a separation between public and private areas gets off to an unclear start. In *Australian Broadcasting Corp v Lenah Game Meats Pty Ltd*[13] Gleeson CJ said:

There is no bright line which can be drawn between what is private and what is not. Use of the term "public" is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford.

11. On the other hand, in *PG and JH v UK*[14] the ECtHR held:

There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectation as to privacy is a significant though not necessarily conclusive factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means at the same public scene (eg…viewing through closed circuit television) is of a similar character. Private life considerations may arise however once any systematic or permanent record comes into existence of such material from the public domain.

12. The Press Complaints Commission Code of Conduct merely notes that:

Private places are public or private property where there is a reasonable expectation of privacy.

13. We can easily distinguish between private and public property, but whether they are private or public places is another matter. Private areas do not automatically ensure privacy, but neither does being in the public gaze necessarily diminish an entitlement to privacy. There undoubtedly is a right to privacy in a public area, but it is a weak right, having less to do with location and more to do with being an

[12] *Bidbay v Spry* 2003 WL 723297 (Cal.App. 2 Dist.)
[13] (2001) 185 ALR 1 cited in *A v B* [2002] 2 All ER 545
[14] *PG and JH v The United Kingdom*, no.44787/98, ECHR 2001-IX

uncertain function of behaviour, expectation and perspective. In life, the degree of privacy we get is dependant on how much we create for ourselves. If we want privacy we lock the door and draw the curtains, erect fences and put up warning signs. On the Internet, we must do the same.

Can the Internet be a "public place" for offences?

14. The dictionary defines "place" in many ways, but within common usage and understanding it could encompass the Internet or parts of it. But this does not necessarily mean that statutes that regulate public place activity would automatically include the Internet. The interpretation of words in statutes has as much to do with context and purpose as literal meaning. English law has a variety of descriptions of what constitutes a public place. In many of these, there is a clear implication within the mischief that the statute seeks to address, that a place must be a geographic location, in order for the nuisance to be physically present, for example a dangerous dog, drunkenness or possession of a weapon. The absence of a physical dimension means that none of these can affect the Internet.

15. However, other "public place" activity, such as indecent display, soliciting or ticket touting, all of which are regulated if conducted on a street, could equally be conducted on the Internet. For the first two examples, it is arguable that the mischief that the law sought to address has, where the Internet is concerned, receded or substantially changed. For ticket touting, contrary to s.166[15] of the Criminal Justice Act 1994, the mischief is two-fold, namely the risk of disorder on the street, and the disruption of preparations to segregate opposing supporters. The latter could occur equally from Internet sales as from touting in the street and therefore the question of whether the Internet is a "place" for the purpose of this law is real.

16. In the case of *R v Hanrahan*[16], the Court of Appeal reaffirmed that "the issue of whether the place was in fact a public place" was a question for the jury. The question for resolution by the judge was whether it was capable in law of amounting to a public place. It would appear that to argue in a case that the Internet is a public place would be a matter of putting sufficient evidence before the judge as to why the website etc. could be a public place, and it then would be a matter for the jury to decide if it is.

What if privacy is breached?

17. Before we go further we should ask the 'so what?' question. Champions of privacy will be disappointed to find that, outside of communications in the course of transmission, UK law provides small certainty and little recourse when privacy is breached. The Human Rights Act 1998, which gives effect to the European Convention on Human Rights, provides no criminal sanction against breaches of privacy. There is no statutory or common law right of privacy, and no tort of invasion of privacy[17], although one is recognised for breached confidentiality. Actions under the Data Protection Act for breaches of an individual's privacy have produced trivial compensation, and no compensation at all can be secured by complaints to the broadcasting and press standards bodies. The absence of proper recourse in the UK was the subject of adverse comment in the ECtHR in

[15] "It is an offence for an unauthorised person to sell, or offer or expose for sale, a ticket for a designated football match in any public place or place to which the public has access or, in the course of a trade or business, in any other place."
[16] Justice of the Peace Vol. 168 4 Dec 2004 p. 947
[17] See *Wainwright v Home Office* [2003] 3 All ER at 966 (para 97)

Peck[18]. Since then judges have said it is a matter for Parliament, and the government have said it is a matter for the courts.

18. Article 8 does not convey an absolute right. It may be breached by public authorities when the law permits, and it must be balanced against rights to freedom of expression under Article 10, enabling journalists and others to breach privacy by citing public interest as justification. Elsewhere, the extent of privacy afforded is governed by the terms and conditions of the relationship. An employee who makes private use of a company's email system is still entitled to privacy in respect of those communications[19] unless the company has reserved the right to monitor employees' Internet usage in its terms and conditions of employment.[20] Internet surfers who believe they are anonymous should check the privacy policy of websites they visit. Many sites, including the Information Commissioner's Office[21], have web analytic mechanisms that include the collection of IP addresses of visitors, which could provide a means of identification. The increased use of broadband and static IP addresses makes this identification easier. Presumably if you disagree with the policy you do not return to the site, but first time visitors discover the policy only after their IP address has been recorded.

19. Society requires public authorities to take action for the common good but there are legal obligations and an overarching moral expectation to go no further than the bare minimum of intrusion into private lives when doing so. We have a watchful press and institutions who challenge the government when they believe the balance is wrong.[22] What are the consequences of law enforcement getting it wrong? In a criminal trial UK law does not require evidence that has been illegally obtained to be excluded.[23] Admissibility is a question of fairness. Judges say that the object of the discretion to exclude evidence under s.78 of PCEA is not to punish the prosecution for transgressions[24], but acts of bad faith by law enforcement officers – "wilfully or knowingly exceeding powers"[25] – have always incurred judicial displeasure. Failure to obtain the appropriate authority may mean the loss of evidence or a halt to the whole proceedings, and could also expose the United Kingdom to international censure, and penalties in the ECtHR.

The control on public authorities

20. The expectation of privacy is multi-faceted, but although Article 8 recognises an individual's right to a private life, it places a mandatory obligation to observe it only on public authorities, albeit that is a very wide class, and the ECtHR has said that the 'essential' purpose of the section is "to protect the individual against arbitrary interference by the public authorities."[26]

21. As already stated, the right is not absolute. Some public authorities, notably law enforcement agencies, may breach that right when it is for the national good and it is lawful to do so. The ECtHR is consistent in pointing out that any surveillance

[18] *Peck v The United Kingdom* [2003] EMLR 15
[19] *Halford v The United Kingdom*, no.20605/92 ECHR
[20] See The Lawful Business Practice Regulations 2000
[21] The Irish Information Commission also records the webpage the visitor was on prior to visiting the IC site.
[22] See Etzioni's argument in *The Limits of Privacy* (Basic Books, New York) on how the development of privacy rights in the US has worked against the development of the common good.
[23] *R v Khan* [1997] AC 558
[24] *R v Hughes* [1994] 1 WLR 876
[25] *Matto v DPP* [1987] Crim LR 64
[26] Case 'Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium' (1968) Series A 6, para 7.

in which private information is gained is a breach of Article 8. That the State properly authorises it to take place does not make it any less of a breach, but it does make the breach lawful[27].

22. In the UK, RIPA provides a statutory framework for surveillance by law enforcement, and requires that surveillance that meets certain criteria – in which an Article 8 breach is likely – be properly authorised. For our purposes we should note that if surveillance (directed surveillance[28]) is planned as part of a specific operation, if it is covert[29] and likely to result in obtaining private information, then the surveillance must be authorised, with due regard paid to necessity[30], proportionality, and the risk of collateral intrusion. Unauthorised directed surveillance may commence as an immediate response to events, with authority being sought when time permits. The Office of Surveillance Commissioners inspects and reviews such authorisations.

23. When covert surveillance is contemplated, the test for UK law enforcement is not to consider the strength of the right to privacy, but merely whether private information is likely to be gathered. It would also include private information from persons whose identity is not known at the commencement of the surveillance, and persons who are not the target of the surveillance. "Private information" for these purposes would appear to include information already in the public domain, and information to which any claim to privacy might be thought to have been waived. In certain circumstances this a very valid concern, one that law enforcement must heed. But on the Internet? How one wishes for *Katz* and the clarity and commonsense of the US position. In *US v Gines-Perez*[31] a defendant sought the exclusion of evidence, on the grounds of breached privacy, because a US Customs officer had downloaded a photograph of the defendant for identification purposes. The photograph was taken from the website of a store where the defendant worked. It was argued that the photograph was private because the website was still under construction. The court thought the claim failed on both elements of the *Katz* test. For the first leg, the subjective test - that the subject should exhibit an expectation of privacy - the judge said

> *A reasonable person cannot place "private" information…on the Internet, if he or she desires to keep such information in actual "privacy." A reasonable person does not protect his private pictures by placing them on an Internet site….*
>
> *But Gines-Perez also fails in the second prong. The Court finds that this society is simply not prepared to recognise as "reasonable" a claim that a picture on the Internet is "private" in nature, such that the Government cannot access it. In fact, the Court believes that our society would recognise the opposite; that a person who places a photograph on the Internet precisely intends to forsake and renounce all privacy rights to such imagery, particularly under circumstances such as here, where the Defendant did not employ protective measures or devices that would have controlled access to the Web page or the photograph itself.*

---

[27] *Perry v The United Kingdom*, 63737/00 ECHR
[28] RIPA s.26.
[29] RIPA s.26(9)(a) The surveillance is covert "if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place."
[30] Authority may only be given for the reasons given in RIPA s.28(3) – these include protecting national security, public health and safety, preventing or detecting crime, and assessing or collecting tax.
[31] 214 F.Supp.2d 205

24. For UK law enforcement, the nub appears to be this. Incidental gathering of information, including private information, whether by request to a third party or from the public domain, for example looking up a subject in *Who's Who,* does not in itself constitute surveillance and so no authority is required. Little objection could be raised where law enforcement uses the Internet to inform itself on issues, groups or personalities. Material published on the Internet may be observed generally by law enforcement. However, if the information collection activity does gather private information and that activity is part of a wider specific investigation then it is no longer incidental, nor an isolated incident, but a part of a larger monitoring exercise and probably will require authorisation.

25. A person committing an illegal act can have no valid claim to privacy in relation to that act[32], and therefore covert surveillance of illegality is not thought to require authorisation. But a question arises: do the observers know that an offence is being committed or merely suspect it to be so? If only the latter, and private information is likely to be gained, then authorisation should be sought. Equally, consideration must be given to collateral intrusion. The test is not the intention, but the possibility that the private information of perhaps unknown innocents may be gathered as part of the operation.

Law enforcement's duty to observe

26. The RIPA Code of Conduct recognises the duty of law enforcement officers to observe generally, and that technology, if an aid to normal sensory perception, may be used in these general observations[33]. A person who steps outside his door knows he is in full view of the public, and any policeman who may be present. However, he has a legitimate expectation not to be put under systematic surveillance unless it is properly authorised. The test is whether the policeman's activity amounts to "monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications."[34] The inference is that watching a new development over a short period of time is OK. Repeatedly returning to watch, or observing over a longer period, particularly when records are kept, becomes monitoring, and is therefore surveillance.

Business affairs

27. As we saw above, the right to privacy may also include activities of a professional or business nature. An individual may expect privacy in his business affairs, but a company or partnership cannot[35] although it can require confidentiality. A legal persona has been thought to lack "the sensibilities, offence and injury to which provide a staple for any developing law of privacy".[36] Gathering information on a company, including monitoring its websites for, say, tax or compliance reasons, would not be a breach of Article 8 as long as the information gathering strategy fell short of gathering private information regarding individuals within the company. The normal expectation is that a commercial website will not contain private information. But if a commercial website is monitored as part of a specific investigation, it is likely that it would have in contemplation either the prosecution of, or the gathering of intelligence on, individuals of that organisation. If this was the case then the association of the individuals to those corporate business

[32] *Ludi v Switzerland* (1992) 15 EHRR 173
[33] RIPA Covert Surveillance Code of Practice paras 1.3, 1.4
[34] RIPA s.48(2)(a)
[35] R v Broadcasting Standards Commission, ex parte British Broadcasting Corporation [2000] 3 All ER 989, 998-999
[36] *ABC v Lenah Game Meats Pty Ltd* (2001) 185 ALR 1

affairs could be deemed to be private information and a directed surveillance authorisation will be needed.

28. Where is the boundary line in an individual's business affairs? At the golf club we may wish to keep private what we do or how much we earn, and others may be uncomfortable about asking, but in other circumstances we may have no reticence at all in making these public. But that is OK because that is our choice. If we advertise our business in a paper or in a newsagent's window, we may reveal personal data, but we can have no expectation of privacy in respect of this information, and we trust to fortune that it is not seen by law enforcement or the taxman, if that were to be a concern to us. We have chosen to put these in the public domain. The same applies if we advertise on the Internet, or offer items for sale on Internet auction sites, and the principle is the same if we choose to publicise our beliefs and opinions in bulletin boards or other open fora. Internet search tools merely assist public authorities in their duty of general observation.

29. But as we have seen above, this is only true of incidental encounters with the material. If the items were to be recorded, to be matched against future searches perhaps to quantify the extent of an individual's business transactions, or to monitor the development of an individual's opinions, then it starts to look like systematic surveillance. In respect of each individual item, it may be that there is no expectation of privacy. But putting these all together to build a bigger picture of an individual's life creates information that could well be private and an authorisation may be required. The fact that at this stage the subject is known only by a nickname is immaterial if there is a prospect that the identity of the subject will be discovered.

Password protection

30. What if the bulletin board in question is not open to the world but behind a password? The protection of a password may not be sufficient to give an expectation of privacy. Following the ruling of Lord Bingham above, does the password genuinely restrict access to a particular group, or can anyone apply and gain access? Passwords are often put there for the protection of the bulletin board owner, and not the users, and the site privacy policy may make clear that no privacy can be expected. Where the forum is genuinely restricted to a particular group, there is strong argument to suggest a user may have consented to reveal private information to a limited circle and no more. He need not anticipate that gatecrashers are present, but he should anticipate that the limited circle might include law enforcement officers who may put their duty before their loyalty to the group. He is, however, entitled to place some reliance on a confidentiality agreement if this is part of the terms and conditions of access. Whether law enforcement needs to seek authorisation prior to access as law enforcement officers is dependant on the particular circumstances of each forum.

31. A distinction should be drawn between passive reading of postings and active participation. The latter may give rise to the creation of a relationship that could make the law enforcement officer into a covert human intelligence source (CHIS), as controlled by RIPA. The Act defines a CHIS as someone who "establishes or maintains a personal *or other* relationship" for the covert purpose "to obtain information"[37]. Two points arise: first, with a CHIS, we are not concerned with just private information. Second, what is meant by covert? RIPA defines a covert purpose as "in relation to the establishment or maintenance of a personal or other

[37] RIPA 2000, s.26(8)

relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose."[38] On the Internet, however, there are many instances where either nicknames or handles are the norm, or where there is little expectation that your correspondent is using his real name. When everyone is openly using false names or identifiers, the abnormal is to use a real name. But the use of a false name is immaterial. The test is whether the underlying purpose is being served by the adoption of a nickname.

Chatrooms

32. A useful analogy might be to compare a chatroom with a public house, or a known criminal hotspot. Plain clothes officers who go to a public house, perhaps a known haunt of criminals, to see what is going on are acting covertly, and the likelihood of obtaining private information (in its widest sense) is high, eg association with others, overheard conversations revealing lifestyle preferences, drinking habits. If the police presence there is not part of a specific operation, then it does not meet the criteria for surveillance that requires prior authorisation. Nevertheless the RIPA Covert Surveillance Code of Conduct suggests that even in non-specific operations, if it is likely that private information may be obtained then authorisation should be sought.[39] As stated earlier, the proper test here therefore is one of the likelihood of private information being obtained, not whether there is a prior intention to eavesdrop or act covertly.

33. The pragmatic assumption that an individual will be less guarded in less public surroundings suggests the issue is best considered as a range with perhaps the confessional or pillow talk at one end and a press conference at the other. At what point on that range does it become likely that private information will be revealed? "Likely" means "real possibility" not "there is an outside chance." The answer still comes back to perspective and expectation. There would appear to be a direct correlation between an individual's reasonable expectation of privacy, and the likelihood of private information being revealed to an eavesdropper, and therefore to a requirement to obtain proper authorisation for directed surveillance, even though the statutory criteria is not met. But it is worth reminding ourselves of the context. It is only public authorities that are bound by this. Private detectives, tabloid journalists and criminals present in the pub do not require authorisation to eavesdrop.

34. But to return to Internet chatrooms. Some participants engage in direct conversation with other users. This has the appearance of a communication in which consent for others to view is implied, but I think this is a false analysis. A user may direct his content to another individual, but he sends his packet to a public place. This is where the analogy of the chatroom and the pub falls down. Users of open chatrooms know that each utterance is not limited to a group of associates around a table but can be viewed by whoever in the world chooses to do so. Commonsense would suggest that participants would not impart information that they wished to keep private, or if it is personal information, it is not information over which they wish to assert Article 8 rights. In addition, if newspapers reflect public opinion – a dangerous assumption I admit – then there is some public support for law enforcement monitoring of chatrooms to protect children. This could be seen as part of the policeman's general duty to observe and prevent crime. However, where the chatroom is genuinely restricted or

[38] S. 26(9)(b)
[39] Covert Surveillance Code of Practice para 2.3

dedicated to a particular interest group then there would be some expectation of privacy within that circle and an increased likelihood that private information could be obtained. Despite the public demand, a directed surveillance authorisation would be required, and CHIS authorisation as well if participation is anticipated.

35. "We are free and tolerant in our private lives; but in our public affairs we keep to the law." So spoke Pericles in his funeral oration for the Athenian war dead. Times change, and if that were true then, it is no longer true today despite it being, for many, a guiding philosophy for life. An Englishman's home is no longer his castle. We no longer accept that in the privacy of our homes we can beat our wives, children and animals and that it is no one else's business. The boundary between public and private, both in law and in perception, changes continually and is often indistinct, but that it exists, and is recognised, maintained and respected, is the key difference between a democracy and a totalitarian state. It is easy to characterise the Internet as the lawless Wild West of communications, but it is also a diligent servant of democracy. It is a vibrant cross-section of life, serving the interests of commerce, individuals, and criminals. As in real life, there is a balance to be struck between effective law enforcement and personal liberty, of which the right to privacy, such as it is, is a part. Recognising that there is a boundary between public and private is an essential part of policing in a democracy, even though that boundary often exists only in perception, and is often disregarded by those it is there to protect.