26. ANONYMITY AND THE LAW IN THE UNITED KINGDOM

IAN LLOYD

I. INTRODUCTION

The wartime British Prime Minister Winston Churchill famously described the government of the Soviet Union as a "mystery wrapped inside a riddle inside an enigma." Attempts to tease legal meaning from the concept of anonymity arouse similar sentiments, and hypothesizing any answers tends merely to give rise to further questions. Like its conjoined sibling privacy, anonymity very seldom enjoys the luxury of dealing in absolutes, and a balancing act has constantly to be struck between competing interests. Trends in social and political thinking also fluctuate over time with greater or lesser stress being placed upon the rights of individuals as opposed to broader claims such as those relating to national security and the prevention and detection of crime."My right to swing a stick," it is suggested, "stops at the point where it hits your head!" In a similar vein, my right to act under conditions of anonymity becomes at least qualified when my conduct impacts upon other people. Anonymity—or at least the ability to operate under a range of false identities—is frequently used by those who wish to make multiple and false claims for social benefits. Data sharing and identity management techniques may be effective in reducing fraud but at the cost of requiring everyone involved to surrender a considerable degree of anonymity.

Increasingly, issues of national security have come to dominate discussion in the field of anonymity in comunications. There is no denying the challenges that modern communications technologies pose for law enforcement agencies.

Encryption tools are available to everyone today at a strength that would have been unimaginable to the largest organizations a decade ago. The volume of text and e-mail messages is such as to swamp any form of real-time interception on the part of law enforcement and national security agencies. Within the United Kingdom, the response has tended to be to require service providers to retain details of all electronic communications for periods considerably beyond those that might be justified by their own operational requirements.

It is difficult to challenge the emotive nature of national security claims. Images of the September 2001 attacks and the more recent bombings in Madrid and London continue to traumatize the Western world. In many respects, the prospects for explicit recognition of a right of anonymity appear bleak, and the current trend is to take away from, rather than add to, rights in this area. The cry "if you have done nothing wrong, you have nothing to hide" is heard with increasing stridency. Warning voices, however, are also being raised. The United Kingdom's Information Commissioner has warned repeatedly against the dangers of "sleepwalking into a surveillance society," and in June 2008 the House of Commons Select Committee published a report on the same topic warning, in particular, of dangers linked to the forthcoming system of identity cards.

II. ANONYMITY AND PRIVACY

The relationship between the concepts of privacy and anonymity is a complex one, and there is a considerable degree of overlap. It might be suggested, however, that the predominant element in any claim regarding privacy is that an individual does not want others to know details of what he or she has been doing. The person striving for anonymity predominantly seeks the freedom to move through public spaces without others knowing who he or she is. Typically, actions alleging breach of privacy are brought by those who might be described as the "rich and famous" whose activities may be of intrinsic interest to many people. Examples include the action brought by the supermodel Naomi Campbell[1] against a newspaper that had published a photograph of her leaving a drug addiction support group meeting and the more recent action brought by the motor racing supremo Max Mosely[2] concerning publicity given by a newspaper about his participation in a sadomasochistic sex session. These cases almost invariably involve a balancing act between the rights of privacy and freedom of expression, with the common complaint made by the media that giving excessive weight to privacy allows the rich and famous to conceal evidence of misdeeds. For most of us, unless we are fortunate or unfortunate enough to enjoy or endure a Warholian

1. *Campbell v Mirror Group Newspapers* [2004] UKHL 22.
2. *Mosely v News Group* [2008] EWHC 1777 (QB).

15 minutes of fame, most of our activities are of limited interest to any other person other than perhaps our nearest and dearest.

III. WHEN IS AN INDIVIDUAL IDENTIFIABLE?

The question of when an individual can be identified—that is, loses anonymity—is one that assumes great importance in the context of data protection legislation. The United Kingdom's Data Protection Act 1998, which is intended to implement the European Data Protection Directive,[3] confers a variety of rights on data subjects and obligations upon data controllers when data relating to a "living, identifiable individual" is processed. If an individual cannot be identified from the manner in which data is collected, processed, or used, there can be no significant threat to privacy and no justification for the application of at least the Data Protection Act—although there may well be rights under other legal headings such as the law of contract or the concept of breach of confidence. The case of *R. v. Department of Health ex parte Source Informatics Ltd.*[4] constitutes an illustration of such a situation. The case involved a challenge to the legality of guidance issued by the Department of Health to general practitioners and pharmacists to the effect that information that had been provided by a patient in confidence was not to be disclosed without the consent of the patient. For the applicant, who was trying to persuade practitioners and pharmacists to allow them to collect anonymous data about prescribing habits, it was argued that the guidance confused the notions of privacy and anonymity. An obligation of confidence, it was argued, could apply only where there was a threat to an individual's privacy, and the applicant argued that the data would be obtained and processed in a manner that would secure anonymity.

The High Court was not convinced. Although it was accepted that most patients would be unconcerned about the use of their data if anonymity was assured, others would be concerned either on the basis of doubts as to the effectiveness of the assurance of anonymity or on the ground that their data should not be used for the commercial advantage of others. In these circumstances, the proposed transfer would constitute the tort of breach of confidence. The Court of Appeal,[5] however, took a different view. Accepting that the data would be transmitted in a form in which they could not be further processed in order to identify individuals, it was held that the purpose of the law was "to protect the confider's personal privacy." The patients did not own the data constituting their prescriptions and in

3. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ 1995 L 281/ 31.

4. *R. v Department of Health ex parte Source Informatics Ltd* [1999] 4 AllER 185.

5. [1999] EWCA Civ 3011.

the absence of anything that might affect their privacy (or anonymity), could have no legal basis to object.

In the case in which data is linked to a named person, there can be no question that the individual is identifiable. A wide range of other identifiers can, however, be envisaged with the European Data Protection Directive stating that:

> an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[6]

Neither the Directive nor the Act provide any definition as to when data relates to an identifiable individual, but the point has been considered extensively by Article 29 Working Party,[7] initially in respect to the privacy implications arising from the use of RFID chips and more specifically to the nature of personal data.[8]

In its initial work, the Working Party suggested that "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated."[9]

Developing this concept in 2007, the Working Party identified three elements that may indicate that data relates to a particular individual. These are referred to as content, purpose, and result elements. The distinction between the elements may be complex on occasion, but the Working Party stresses that only one element needs to be present in order to justify a finding that data relates to a particular individual. The content element will be satisfied when information is about an individual. A medical or personnel record, for example, will fall within this category. The purpose element applies when the data is intended to be used to determine the manner in which an individual is treated. Data may, for example, be recorded by an employer of the Web sites accessed from workplace computers. The purpose may be to take disciplinary action against employees who violate Internet usage policies. Finally, a result element applies when the use of data, even though not collected originally for that purpose, is likely to have even a minor impact upon an individual's rights and interests. Further guidance produced by the United Kingdom's Information Commissioner emphasizes similar criteria suggesting that:

> Data which identifies an individual, even without a name associated with it, may be personal data where it is processed to learn or record something

6. Article 2(a).

7. The Article 29 Working Party was established under that article of the directive and is effectively a committee of all national data protection supervisory agencies.

8. Working Paper 4 of 2007.

9. Working Party document No WP 105: "Working document on data protection issues related to RFID technology," adopted on 19.1.2005, p. 8.

about that individual, or where the processing of that information has an impact upon that individual.[10]

Once again the Article 29 Opinion identifies a wide range of potential situations and provides extensive guidance. Linking data to a name is an obvious form of identification, although especially in the case of a common name such as Smith or McDonald, this may not sufficient. Use of an identification number may aid identification. In other cases an individual may be identifiable indirectly. The example might be posited of a closed circuit television camera (CCTV) operator instructing an undercover police officer to "detain the person wearing a Glasgow Rangers' football shirt and carrying a can of lager sitting slumped in the doorway of 27 Hoops Street Glasgow." No name is given, but the individual is readily identifiable. Again ISPs and possibly employers may maintain records of Internet use associated with particular computers and from these to the individuals behind the computers.

The work of the Article 29 Working Party is significant and illustrates well the blurring of divisions between privacy and anonymity. Given the increasing sophistication of data processing technologies, the individual's sense of anonymity may be compromised even in cases in which identification by name is not possible.

IV. RECOGNITION OF ANONYMITY AS A HUMAN RIGHT?

The European Convention on Human Rights has had a direct effect in the United Kingdom since the enactment of the Human Rights Act 1998. Effectively, any person can claim before a court that rights established under the Convention have not been respected and demand that the court provide a remedy.

The Convention, in common with almost every national and international instrument, makes no specific reference to a right of anonymity. Neither, it might be noted, does it establish a specific right of privacy. Instead recognition of rights can be seen as implicitly recognized in a number of articles of the Convention, principally although not exclusively, articles 2, 3, and 8.

Article 8 is of the most direct relevance and requires respect for an individual's private and family life, home, and correspondence. This is frequently referred to, not least in the dicta of the European and national courts, as conferring a right of privacy, although this is only one component of what has been accepted as a very broad-ranging right.

10. "Determining Personal Data—Quick Reference Guide," Available from <www.ico.gov.uk/upload/documents/library/data.../160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf>.

This provision has been at issue before the United Kingdom and European courts on many occasions. Two cases are of particular significance to the present chapter. In *Peck v. United Kingdom*, the claimant had been seen by the operators of a local authority's CCTV system walking in the streets in a distressed condition and carrying a large knife. The police were alerted and discovered the claimant in the act of attempting to cut his wrists. The incident was reported in the local authority's newsletter as evidence of the success of the CCTV system, and subsequently a number of broadcasters sought copies of the footage. Although it appears that the authority obtained a verbal undertaking that the claimant's features would be masked when the material was broadcast, this did not take place. Failure to ensure anonymization of the data was held by the European Court of Human Rights to constitute a breach of the claimant's Article 8 rights.

The decision in *Peck* came from the European Court of Human rights and was delivered prior to the implementation of the Human Rights Act within the United Kingdom. The recent decision of the Court of Appeal in the case of *Murray v. Big Pictures*[11] provides an illustration of the application of these principles under domestic law. At issue were a number of photographs taken surreptitiously of the well-known author J. K. Rowling, her husband, and infant son walking (or in the case of the son, being pushed in a buggy) along a public street. An action raised on behalf of the child sought an order, based on rights conferred by Article 8 of the Convention, that the photographs be handed over. At trial, the action failed, in large part because the judge assumed that the claim being raised on behalf of the child was merely a smoke screen for an attempt to protect the mother in circumstances in which she would have no actionable right to privacy, as all aspects of the case had taken place on a public street. The Court of Appeal was more sympathetic. As in so many aspects of life, context was critical. If a photograph had been taken as a "street scene" and subsequently published, there could have been no cause for complaint. In the present case, however, the defendant had deliberately sought to capture the image secretly and with the intention of profiting from its use. Although any publication of an image must carry the risk that someone will identify the individuals portrayed, the key element of the Court's decision would appear to be that when anonymity is deliberately destroyed without due cause, an action will lie under Article 8.

In addition to Article 8, account has to be taken also of a number of other provisions of the European Convention on Human Rights, in particular, Articles 2 and 3. These provide respectively that:

> Everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court . . . No one shall be subjected to torture or to inhuman or degrading treatment or punishment.

11. *Murray v Big Pictures* [2008] EWCA Civ 446.

The major case on this point is that of *Venables and Thompson v. News Group Newspapers and Others*.[12] Here, the claimants had a number of years previously been convicted of the murder of a young child. At the time they were both ten years old. Although their identities had been concealed during the trial, subsequent to their conviction the judge directed that their names and some of their background should be made public. Injunctions were also issued, however, prohibiting the publication of further information in order to facilitate the possibility that the individuals might be rehabilitated and reintegrated into society.

By 2000 the claimants were reaching eighteen years old, and the initial injunctions would have expired on their birthdays. The likely date of their release from custody was expected to be in 2001, and arrangements were in hand to provide the claimants with new identities. Proceedings were brought by them seeking continuance of the injunctions in perpetuity out of fear that, once released into the community, their lives would be at very real threat should their identities be disclosed.

The murder in question had been a particularly horrific one, and evidence indicated that feelings within the public at large (and relatives of the deceased in particular) still ran very high. A variety of media reports were put before the court. One entitled "Throw Away the Key" suggested that:

> . . . if Venables and Thompson returned to Liverpool they would be lynched—and nobody would shed a tear. The pair of them should stay inside for the rest of their natural lives. They took a baby's life. So why should they be allowed a life of their own?[13]

Faced with such evidence the court was driven to the

> . . . inevitable conclusion . . . that sections of the Press would support, and might even initiate, efforts to find the claimants and to expose their identity and their addresses in their newspapers.[14]

The media claim to publish information under the protection of Article 10, therefore, could not compete with Article 2 and 3 protections. Injunctions were granted prohibiting, *inter alia*, the publication of any information likely to lead to the identity of the claimants.

In some respects this case is an exceptional one, and in only one other case[15] has a similar injunction been issued. The issue of publication or retention of details of criminal convictions is a rather broader one, and significant publicity has attended attempts by some media outlets to publish details of the name and

12. *Venables and Thompson v News Group Newspapers and Others* [2001] EWHC QB 32.

13. Part D para 12.

14. At Part E para 4.

15. *X (A Woman Formerly Known As Mary Bell) & Anor v O'brien & Ors* [2003] EWHC 1101 (QB).

current address of persons convicted of sexual offences involving children. In a recent case,[16] the Information Tribunal has ruled that the retention by the police of details of minor convictions many years in the past contravenes the requirement of the Data Protection Act that data should not be retained beyond a reasonable time.

V. ANONYMITY IN THE CRIMINAL JUSTICE SYSTEM

The previous discussion has concerned the possibility that convicted criminals may be afforded a measure of anonymity in order to rehabilitate themselves into society. The issue of anonymity is currently a matter of major controversy at an earlier stage of the criminal justice process with debate concerning the possibility that witnesses in criminal cases may be permitted to give evidence under conditions of anonymity. The recent decision of the House of Lords in the case of *R v. Davis*[17] has generated massive publicity and the enactment of emergency legislation by parliament to overturn most aspects of the decision.

The principle that all aspects of court proceedings should be conducted in public has been a fundamental tenet of the United Kingdom's criminal justice system for centuries. In a number of high-profile cases of serious crime or terrorism, difficulty has been encountered in persuading witnesses to give evidence out of fear of the consequences should they be identified by defendants or their associates, and measures have been taken by the courts under common-law powers to preserve the anonymity of witnesses.

In *R v. Davis*, the appellant had been accused of murder. A number of potential witnesses had indicated to the authorities that they would fear for their lives should they be identified as giving evidence. To induce them to testify, the trial judge, exercising common-law powers, made a series of orders under which they could give testimony under pseudonyms and shielded from the sight of the public and of the accused and his legal advisers, that their voices should be electronically modulated, and that the accused or his counsel should not be permitted to know details of the witnesses or to ask any questions in cross examination that might lead to their identification.

Following trial, the accused was convicted. The conviction was upheld by the Court of Appeal but overturned by a unanimous decision of the House of Lords. Delivering the leading judgment, Lord Bingham restated the principle that an accused was entitled to be confronted by his accusers in open court "in order that he may cross examine them and challenge their evidence."[18] After surveying a

16. *Chief Constable of Humberside and Others v Information Commissioner*, 21 July 2008, http://www.informationtribunal.gov.uk/Decisions/dpa.htm.

17. *R v Davis* [2008] UKHL 36.

18. At para 5.

wide range of authorities from a number of common-law jurisdictions and recognizing that exceptions had validly been made to this principle in cases—for example, when a witness had died prior to trial—Lord Bingham concluded that the level of anonymity granted to the witnesses had unlawfully deprived the appellant of his right to a fair trial. Although some limited exceptions to the general requirements of openness might be acceptable in specific cases, the grant of absolute anonymity contravened the principles of common law. Accordingly the conviction was quashed with clear signals sent to the government that if this result was seen as unsatisfactory, it was for Parliament to change the law rather than for judges to violate basic tenets of common law.

Change did follow after dire predictions from law enforcement agencies concerning the number of serious crimes that could not realistically be prosecuted unless witnesses could be assured of anonymity. Up to forty convicted criminals, it was suggested, might also be able to appeal their convictions.[19] The Criminal Evidence (Witness Anonymity) Act received the Royal Assent on July 21, 2008, only thirty-three days after the decision of the House of Lords. The Act repeals all common-law powers regarding the grant of anonymity[20] and provides for the making of "witness anonymity orders."[21] These may be made by a court when it is considered appropriate and when they effectively provide for measures similar to those considered unacceptable in Davis.

VI. SURVEILLANCE AND THE DEMISE OF ANONYMITY

A range of statutes provides the legal basis for surveillance in the United Kingdom. The Regulation of Investigatory Powers Act 2000 is the major statute, but this has to be considered in conjunction with the Anti-Crime and Terrorism Act of 2001,the Intelligence Services Act 1994, and the Security Services Acts of 1989 and 1996. The combined statutes provide legal sanction for a wide range of covert information-gathering activities as well as for access to a wide range of communications data. The Regulation of Investigatory Powers Act provides for the issuance of warrants legitimizing covert surveillance. These extend beyond interests of national security or even serious crime and may be invoked by a range of organizations including local authorities.

A recent survey conducted by the Press Association asked ninety-seven local authorities for details of their use of surveillance powers. Forty-six authorities responded, describing 1,343 uses of the powers. Most surveillance was directed against instances of suspected fraud, but there was also evidence of the use

19. "Police Chief Fears Witnesses Rule," BBC News Channel, June 21, 2008, http://news.bbc.co.uk/1/hi/uk/7466946.stm.

20. Section 1(1).

21. Section 2.

of powers to detect persons allowing their dogs to foul public areas, who left litter in the streets, or misused parking spaces marked for the use of disabled persons.[22]

Activities such as those previously cited constitute a worrying indication of how widespread are the use of powers permitting surveillance activities in respect to what may be regarded as minor infractions of the law. It is at this level that we again see the complex relationship between notions of privacy and anonymity. Monitoring of everyday activities such as dog walking goes beyond concepts of privacy, which are concerned primarily with bringing unusual or noteworthy conduct into the public arena. We cannot expect to walk a dog in a public place without being noticed, but the sense that the activity (or any other act taking place in public) is the subject of targeted observation instills a sense of disquiet in many people, relating more to a sense of loss of anonymity than to privacy. This is the case even though we may not be identified by name. As was discussed above in the context of data protection, identity is about much more than names.

A. Use of CCTV as a Surveillance Tool

Although many of the instances of surveillance carried out under the Regulation of Investigatory Powers Act make use of human agents, this form of activitity is expensive, especially in terms of the number of watchers required. Increasingly, surveillance technologies are being automated. Perhaps the most noticeable and extensive surveillance tool is the closed circuit television camera (CCTV). It is a rare high street or even shop that does not have one or more cameras. It is estimated that there are approximately 4.2 million CCTVs in the United Kingdom. With a population approaching 60 million, that equals one camera for every fourteen inhabitants of the country. Two million motorists are fined each year as a result of being caught by speeding cameras. In general it is estimated that the average person can expect to be "caught" on camera around 300 times a day.[23]

Traditionally, CCTV systems have relied upon images being viewed and assessed by human operators. In at least some instances, this is no longer the case. A nationwide system of Automatic Number Plate Recognition cameras is being installed on the United Kingdom's roads and is scheduled for completion in 2008, at which time about fifty million number plates will be recorded each day.[24] The cameras will capture images of car number plates and compare these with records maintained by the Driving and Vehicle Licencing Agency and motor insurance companies to identify vehicles that are not taxed or insured.

22. "Spy Law Used in 'Dog Fouling War,'" BBC News Channel, April 27, 2008, http://news.bbc.co.uk/1/hi/uk/7369543.stm.

23. "Britain is 'Surveillance Society,'" BBC News, November 2, 2006, http://news.bbc.co.uk/1/hi/uk/6108496.stm.

24. "Your Life in Their Lens," *Telegraph*, November 3, 2006, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/11/02/nspy202.xml.

The system will also link with police databases to flag the appearance of any vehicle recorded as being of interest to the police.[25]

VII. ANONYMITY IN ELECTRONIC COMMUNICATIONS

A walk down any street will evidence the fact that for many people, electronic communications have become an indispensible part of life. Although use of mobile phones in public places affords very little privacy (either for the caller or for others in the vicinity!), there is normally the sense of anonymity. Additionally, e-mail has to a very large extent supplanted the postal system as a means of communication.

The Regulation of Investigatory Powers Act 2000 empowers a senior police officer to require a communications provider to disclose any communications data in its possession when this is considered necessary in the interests of national security, the prevention or detection of a crime, or a number of other situations.[26] The term "communications data" is defined broadly to include any data relating to a communication other than the contents of the communication itself. Thus details of numbers called (whether answered or not), time and duration of calls, e-mail addresses, and the URL's of Web sites visited are consider communications data. Also included is "location data," in the form of information relating to the location (and movements) of a mobile phone.[27]

The procedures to be followed in requesting or requiring disclosure are laid out in a Code of Practice on the Acquisition and Disclosure of Communications Data, which was brought into force by the Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order 2007.[28]A wide range of public authorities can lawfully access communication data—from the police through to the Department of Transport (DoT). It has been stated by the Home Office that "Law enforcement

25. Details of the system and its possible uses are given in a document, "ANPR Strategy for the Police Service 2005–8" produced by the Association of Chief Police Officers and available from www.acpo.police.uk/asp/policies/Data/anpr_strat_2005-08_march05_12x04x05.doc.

26. Section 22.

27. See "Mobile Phones Expose Human Habits," BBC News, June 4, 2008, http://news.bbc.co.uk/1/hi/sci/tech/7433128.stm.

28. SI 2007 No. 2197. for an interesting account of the use of location data to track the movements of 100,000 mobile users (under conditions of anonymity) as part of research work designed to identify the nature of human movements. One conclusion was that the majority of people seldom moved more than 10 kilometres from home.

agencies make roughly half a million requests for communications data annually."[29]

Under the 2000 Act there was no obligation upon service providers to retain traffic data, and indeed the Data Protection Act 1998 requires that data be retained for no longer than is necessary for the purpose for which it was first processed.[30] The extent of time might vary depending upon the nature of the communication and the nature of the communications provider's relationship with the user. In a situation in which a mobile phone was supplied under a contract providing for bills to be sent each month, it would be reasonable for the provider to retain the data until the bill had been accepted as accurate by the customer and payment received. For prepaid customers, it would be difficult to justify retention for more than a very short period of time.

A further statute, the Anti-Crime and Terrorism Act of 2001, was rushed through parliament in the aftermath of September 11 and provided power to the Secretary of State to issue a code of practice defining the length of time that service providers might lawfully retain traffic data for the purposes of the Regulation of Investigatory Powers Act.[31] Such a code was issued in 2003,[32] and its Appendix A specifies the periods of time that various forms of data might lawfully be retained. In most cases a period of six months is laid out,but in the case of Web activity logs (restricted to the first page of a Web site) the period is reduced to fourdays.

The 2003 code legitimized rather than mandated data retention. This situation changed upon the implementation of the European Directive "on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks"[33] (the data retention directive). This directive, which was introduced in the aftermath of the Madrid and London bombings in 2004 and 2005, respectively, provides in Article 5 that service and network providers are to be required to retain a very wide range of items of communications data relating to the source and destination of telephone calls, e-mails, and Internet access. The directive provided that member states might opt out of applying its provisions to all the forms of communications listed and the United Kingdom, along with a number of other states issued a declaration to the effect that

> it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.[34]

---

29. "Communications Data," Home Office Security, http://security.homeoffice.gov.uk/ripa/communications-data.

30. Fifth data protection principle. Schedule 1.

31. Section 102.

32. Available from http://security.homeoffice.gov.uk/ripa/communications-data/retaining-data.

33. OJ 2006 No L105/54.

34. *Ibid.*

The periods for which items of data are to be retained are to be specified by member states within the range of sixmonths to two years. The directive was implemented in the United Kingdom by the Data Protection (EC Directive) Regulations 2007,[35] which entered into force on October 1, 2007. Regulation 5 requires that communication data must be retained for a period of twelve months.

VIII. ANONYMITY AND THE INTERNET

The Internet is frequently, although erroneously, touted as a haven for anonymity. As with any other environment, the Internet can be used for lawful or for unlawful purposes. An example of the latter might be forms of file sharing that constitute infringement of copyright in musical or other works. Again, individuals may use the apparently anonymous nature of the Internet to post comments that are defamatory of another person. In the event that legal proceedings ensue, posters may discover that anonymity is more apparent than real.

In *Totalise v. Motley Fool Ltd.*[36] a company, Interactive Investor, operated a business providing financial information to individual investors. The information was made available via a Website. Included in the Website was a bulletin board facility allowing users to post views and comments.

In order to access the Website, users had to register and indicate acceptance of the operator's terms and conditions. These contained a data protection notice to the effect that the provider would not pass personal data on to any other parties.

One user, operating under the pseudonym "Zeddust," posted comments that were defamatory of the claimant company. The latter complained to Interactive, who removed the positing and suspended the user. Totalise then requested provision of information identifying the poster in order to initiate proceedings for defamation. This was refused by Interactive, who stated that the supply of personal data would place it in breach of its terms and conditions and also of the requirements of the Data Protection Act 1998.

Procedurally the case involved complex questions as to costs and turned on whether the defendant had acted unreasonably in refusing to divulge the identity of its users without need for the claimant to obtain a court order. The Court of Appeal held that the behavior was not unreasonable. The issues involved, it was ruled, were complex, especially with the addition of the Human Rights Act 1998 to the UK statute book. A balance had to be struck between the interests of the claimant in being able to secure a remedy and the respect for the private life of

35. SI 2007 No 2199.
36. *Totalise v Motley Fool Ltd* [2001] EWCA Civ 1897, [2002] 1 WLR 1233.

the individual. In such a situation, it was not unreasonable for a party to refuse to hand over the information on a voluntary basis in the absence of consent from the individuals concerned. The issue could reasonably, it was held, be left to the court to decide, with the Web site owner taking what was referred to as a "neutral" position with regard to the claimant's demands.

Further consideration was given to these issues in the case of *Sheffield Wednesday Football Club Ltd. and Others v. Hargreaves.*[37] The claimants here were parties connected with the management of a less-than-triumphant English football club. The defendant operated a supporters' Web site that allowed for the posting of comments on matters concerned with the club. A number of comments (published pseudonymously) were considered to have been defamatory of the claimants, who brought an action before the courts seeking an order that the Web site owner identify the individuals responsible (users were required to register with the site owner before being allowed to post comments).

The basis for the action (as was also the case under *Totalise v. Motley Fool*) lay under the doctrine laid down by the House of Lords in the case of *Norwich Pharmacal Co. v. Commissioners of Customs and Excise.*[38] This established the doctrine that a party to potential litigation could seek disclosure of information held by a third party that might identify others against whom a claim could be made if three conditions could be satisfied:

- A wrong had arguably been committed against the claimant by a third party whose identity was not known to the claimant.
- Identification of the third party is necessary to allow proceedings to be instituted.
- The party against whom the action is brought must be in a position to identify the wrongdoer.

Although these conditions will normally be met in a case involving Internet bulletin boards, it was emphasized that the court retained the discretion whether to make such an order. As is common in discussion groups devoted to participants' enthusiasms, many of the postings in question, although technically defamatory, were insulting rather than damaging. The judge described several of the comments as being "trivial" or amounting to no more than "saloon-bar moaning about the way in which the club is managed." In these cases, the court declined to order the identification of the posters. In other instances, complaints centered on allegations of financial impropriety, and in these cases it was held that disclosure should be made.

Once again, a balancing act has to be performed between notions of free speech and the interests of the subject of material not to have their reputation or

37. *Sheffield Wednesday Football Club Ltd and Others v Hargreaves* [2007] EWHC (QB) 2375.

38. *Norwich Pharmacal Co v Commissioners of Customs and Excise* [1973] 2 AllER 943.

financial interests damaged. The approach of the court in *Sheffield Wednesday* is to be welcomed in recognizing that the full might of the law should not be used against those who engage in what might be regarded as robust criticism in a forumin which this can cause little genuine harm to the subject. In other cases, matters may take a different aspect. In 2008, an agreed award of £100,000 damages, possibly the largest award in a case of Internet defamation, was made in respect to the activities of a Web site, Dads Place. In a statement to the court it was recounted that

> this group were responsible for the publication of a seriously defamatory, abusive and scurrilous anonymous website at www.dadsplace.co.uk . . . Over a period of two years from April 2004 to about mid-July 2006, from behind their cloak of anonymity, Dads Place used their publications and in particular the Website to conduct a malicious, unpleasant and relentless campaign of libel and harassment.[39]

It appears that the Website was established by one of the defendants, a property developer, to pursue a personal and professional vendetta against a rival company and its managing director. Few could argue in support of a right to anonymity when conduct is so malignant in nature and, as indicated in court, had such damaging consequences for the personal and professional lives of those targeted.

A rather different aspect of Internet-based activities concerns the attempts by parties to monitor these activities through placing devices commonly referred to as "cookies" on users' computers. Cookies can take a variety of forms and persist for periods of time ranging from seconds to, potentially, centuries. Effectively, cookies store data relating to browsing activity and pass this data to their controller. At one level, cookies might be used by e-commerce Web sites to allow them to recognize previous customers and to personalize the data presented to them; in other cases the intention may be to build a profile of an individual's or (perhaps more accurately) an individual computer's browsing habits.

European and United Kingdom legislation applies to the use of cookies with the European Communications Data Privacy Directive,[40] providing that the use of cookies should be lawful only when this occurs with the consent of users. The major difficulty may well be that the default setting of Internet browsers such as Microsoft Explorer is set to accept cookies. In many cases even if the user changes the setting either to require notice of and approval for the placing of a cookie or to refuse to accept any cookies, the effect will be to render access to many Websites difficult or even impossible. For users the choice may be between accepting cookies or doing without access to a site. In such cases consent might not be considered either informed or freely given.

---

39. www.gentoogroup.com/pdf/Statement_in_Open_Court.pdf.
40. Directive 2002/58/EC.

IX. USE OF BIOMETRIC BANKS FOR LAW ENFORCEMENT PURPOSES

The United Kingdom operates what is reported to be the world's largest DNA database used for law enforcement purposes. As of December 31, 2007, data relating to almost five million individuals was held,[41] with this figure increasing by around 700,000 every year[42]. The database per se has no statutory basis, but a range of statutes dating back some ten years has increased both the range of situations in which the police are entitled to take DNA samples and the use to which these may be put. Essentially in England and Wales, samples may be (and are) taken whenever an individual is arrested for a "recordable offence." This covers all but the most minor offences. Once taken the DNA may be retained on the database without limit of time, even when no conviction is subsequently secured. The situation differs in Scotland, where DNA must be destroyed in the event that the individual is acquitted of the charge in respect of which the sample was taken. The conformity of the English practice with the requirements of Articles 8 and 14 (prohibition against discrimination) was tested before the courts in the case of *R v. Chief Constable of South Yorkshire Police ex parte LS and Others*[43] and was upheld by a majority of the judges in the House of Lords. Delivering the leading judgment for the majority, Lord Steyn endorsed the comments of Lord Justice Sedley in the Court of Appeal. Considering the application of Article 8, he commented that:

> The purposes of retention—the prevention of crime and the protection of the rights and freedoms of others to be free from crime—are four-square within Article 8(2), and retention is provided for by law.[44]

As regards the Article 14 claim, the argument was that there was discrimination between those who had been charged but not convicted of an offence (and therefore had to be presumed innocent) and those other innocent persons who had not come to the notice of the police. This claim was also rejected. First it was accepted that any difference in treatment was a result of history rather than status. An analogy was drawn with a person who may have suffered a broken leg and had x-rays taken in a hospital. The fact that these might be retained would not be compromised by the fact that individuals who had not suffered similar misfortune would not have had their details recorded. Rather more contentiously, Lord Steyn also failed to overturn a further argument put forward by Lord Justice Sedley in the Court of Appeal to the effect that:

> The line between those unconvicted people who have faced charges and those who have not, while not a bright line, is not arbitrarily drawn. It does

41. House of Commons Select Committee on Home Affairs, May 20, 2008.

42. http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070510/text/70510w0019.htm.

43. *R v Chief Constable of South Yorkshire Police ex parte LS and Others* [2004] UKHL 39.

44. [2002] EWCA Civ 1275 at para 69.

> not tarnish the innocence of the unconvicted in the eye of the law. But it recognises that among them is an indeterminate number who are likelier than the rest of the unconvicted population to offend in the future or to be have found to have offended in the past.[45]

It has recently also been reported that:

> Primary school children should be eligible for the DNA database if they exhibit behaviour indicating they may become criminals in later life, according to Britain's most senior police forensics expert.[46]

The notion that there are categories of innocence seems to contradict basic tenets of the law to the effect that an individual is presumed innocent until found guilty. Following the maxim that there is no smoke without fire may be appropriate for a writer of crime fiction but should have no place in a mature legal system.

Given the current scale of the DNA database and its claimed utility[47] as a tool for crime detection, there is pressure from some sources for further expansion. There seems no doubt that a disproportionate percentage of persons from disadvantaged backgrounds and areas have their DNA currently held. Perhaps paradoxical argument is that the present system of partial coverage is discriminatory against such persons and that a system of universal inclusion, perhaps from birth, should be instituted. When such a solution was advanced by Lord Justice Sedley, the government response was that "we are broadly sympathetic to the thrust of what he has said."[48] Once again we see the dilemmas that flock to every facet of the topic. Universal DNA testing may well prove an effective tool for the purposes of criminal investigation. Selective testing involving loss of anonymity for some but not others is difficult to defend conceptually. Perhaps the major flaw in the UK system is that, as noted at the start of this section, the DNA database has grown in an ad hoc fashion with very little in the way of parliamentary discussion, let alone legislation.

X. CONCLUSIONS

In the Bible, we are told "vanity, vanity, all is vanity." The term "inconsistency" could well be substituted for "vanity" in the present context. Different interests

45. [2002] EWCA Civ 1275 at para 86.

46. "Put Young Children on DNA List, Urge Police," *The Observer*, March 16, 2008, http://www.guardian.co.uk/society/2008/mar/16/youthjustice.children.

47. It is claimed (*The Independent*, September 5, 2007) that 3,500 matches are provided to police forces each month. It has also been claimed that although only 14% of cases of burglary are solved by traditional policing methods, the figure rises to 48% when DNA evidence is obtained at the scene of crime.

48. "Judge Wants Full DNA Base," Manchester Evening News, September 5, 2007, www.manchestereveningnews.co.uk/news/s/1015525_judge_wants_full_dna_database.

and people have different expectations, and it is perhaps fair to suggest that most of us display internal inconsistencies. We claim to value privacy and anonymity, yet millions of British householders have signed up for store loyalty cards, which provide a key to link massive amounts of personal data relating to our shopping patterns. Again, millions of people voluntarily disclose personal information to social networking Web sites either unaware or uncaring of the consequences, which may follow them for the rest of their lives. Law can only do so much. It is fair criticism that too little has been done to create a framework for a right of anonymity, but all too often people fail to take even the most elementary steps to protect themselves.