Lecture

SINGAPORE ACADEMY OF LAW ANNUAL LECTURE 2015 – "IS NOTHING SECRET? PRIVACY AND CONFIDENTIALITY, PRIVACY, FREEDOM OF INFORMATION AND WHISTLEBLOWING IN THE INTERNET AGE"

The Right Honourable the Lord **NEUBERGER** of Abbotsbury*
President of the Supreme Court of the United Kingdom.

I. Introduction

1 It is a signal honour to be invited to give this lecture, especially in Singapore's 50th anniversary year. Since 1965, Singapore has come an impressively long way from being a little-known speck on the map at the bottom of the Malaysian peninsula. You have a government, which, according to the highly respected *Economist* magazine, "hold[s] [itself] to high standards", and you have become "the world's only fully functioning city state", with a "diversified economy with a strong manufacturing base as well as many service industries", low unemployment, and "a structural surplus [which represents] a higher proportion [of GDP] than any other developed economy".[1]

2 I know from first-hand experience of the high quality of your judges from their judgments which come to our attention in the UK Supreme Court. We recently followed[2] what we called "an impressively wide-ranging judgment"[3] given by your Chief Justice[4] on the subject of passing off (*ie*, marketing goods and services giving the impression that they are someone else's). The appellant claimed that the reputation it

* I should like to thank Hugh Cumber of 5 Stone Buildings Lincoln's Inn and Liu Zhao Xiang of Singapore for their invaluable assistance in preparing this talk. I should also express my debts to the editors of and contributors to *Emerging Challenges in Privacy Law: Comparative Perspectives* (Normann Witzleb *et al* eds) (Cambridge University Press, 2014), as well as to David Anderson QC for his report, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015).

1 Simon Long, "Special Report: Singapore – The Singapore Exception" *The Economist* (18 July 2015) at pp 2, 1, 7 and 7 respectively.

2 *Starbucks (HK) Ltd v British Sky Broadcasting Group plc* [2015] UKSC 31; [2015] 1 WLR 2628.

3 *Starbucks (HK) Ltd v British Sky Broadcasting Group plc* [2015] UKSC 31; [2015] 1 WLR 2628 at [45] and [66].

4 *Staywell Hospitality Group Pty Ltd v Starwood Hotels & Resorts Worldwide Inc* [2014] 1 SLR 911.

had built up in the UK through merely advertising its services meant that it had enough of a reputation to bring a passing off claim. This was inconsistent with established principles, but the appellant argued that we should change the law because of developments in IT, and in particular the Internet. We rejected that, saying:[5]

> … given that it may now be so easy to penetrate into the minds of people almost anywhere in the world so as to be able to lay claim to some reputation within virtually every jurisdiction, … the imbalance between protection and competition which [the appellant's] case already involves … would be exacerbated.

II. Privacy is a fundamental right

3 The effect of the Internet on legal rights is central to my talk today. However, the right in question, privacy, is perhaps more fundamental than any intellectual property ("IP") right, although it has only relatively recently been recognised in law. Today, most international conventions on human rights and liberties now protect the right to privacy.[6]

4 As was famously said 45 years ago, "[a] man without privacy is a man without dignity".[7] Indeed, simply knowing that your actions and words are, or even may be, heard or seen by others affects what you say and do. The 18th-century philosopher Jeremy Bentham designed a

---

5 *Starbucks (HK) Ltd v British Sky Broadcasting Group plc* [2015] UKSC 31; [2015] 1 WLR 2628 at [63].

6 Universal Declaration of Human Rights (10 December 1948) Art 12; United Nations Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (18 December 1990; entry into force 1 July 2003) Art 14; United Nations Convention of the Rights of the Child (20 November 1989; entry into force 2 September 1990) Art 16; International Covenant on Civil and Political Rights (16 December 1966; entry into force 23 March 1976) Art 17. Provisions in regional conventions include Art 10 of the African Charter on the Rights and Welfare of the Child (OAU Doc CAB/LEG/24.9/49) (entry into force 29 November 1999); Art 11 of the American Convention on Human Rights (22 November 1969; entry into force 18 July 1978); Art 4 of the Declaration of Principles on Freedom of Expression in Africa (17–23 October 2002); Art 5 of the American Declaration of the Rights and Duties of Man (2 May 1948); Art 21 of the Arab Charter on Human Rights (22 May 2004; entry into force 15 March 2008); and Art 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950; entry into force 3 September 1953). See also Johannesburg Principles on National Security, Free Expression and Access to Information (1 October 1995) and Camden Principles on Freedom of Expression and Equality (April 2009). This list is taken from the Privacy International website: <https://www.privacyinternational.org>.

7 Zelman Cowan, "The Private Man" (1970) 24 Inst Pub Affairs Rev 26. He went on to say that "the fear that Big Brother watching and listening threatens the freedom of the individual no less than the prison bars".

prison where all the prisoners could be under observation at any point. He described it as "a new mode of obtaining power of mind over mind, in a quantity hitherto without example".[8]

5 However, even the identity and nature of fundamental rights may vary with time and place. Virtually every fundamental right which most people in the UK would take for granted today would not have been seen as a right at all by anyone in England 400 years, let alone 800 years, ago, when Magna Carta was sealed.[9]

6 A wide-ranging new law in France, with its relatively *dirigiste* tradition, seems to have prompted a relatively muted response, whereas in Germany, with its memories of the Nazis and the Stasi, a proposed new law, which is probably less intrusive,[10] has caused much outrage.[11]

III. Privacy is a qualified right

7 While it is vital, the right to privacy has to be subject to constraints. Perhaps the most frequently encountered constraint is when privacy comes into conflict with another, perhaps even more important, and qualified, right, freedom of expression. Partly because it is the media who most frequently question the right to privacy, at least in the UK, we may overlook the fact that, in many ways, the right to privacy is an aspect of freedom of expression. Most people would feel very constrained about what they felt free to say or do on social, family or even many business occasions if they knew that their words or actions would or even might be broadcast generally.

8 An equally important tension exists between privacy and national security and law enforcement. The extent of the tension is no better demonstrated than through the contrasting public reactions to the revelations published by Edward Snowden. Condemnation and praise are handed out in almost equal measure by journalists and political commentators – and with almost equal vehemence and one-sidedness. A balanced and thoughtful analysis of the tension between national security and privacy can be found in the report[12]

8 Jeremy Bentham, *The Works of Jeremy Bentham* vol 4 (William Tait, 1843) at p 39.

9 Although privacy was recognised in some ancient texts as pointed out by David Anderson in his review, David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) at para 2.3.

10 Kim Willsher, "France Approves 'Big Brother' Surveillance Powers Despite UN Concern" *The Guardian* (24 July 2015).

11 Matthew Karnitschnig, "NSA Flap Strains Ties With Europe" *The Wall Street Journal* (9 February 2014).

12 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015).

published a couple of months ago by David Anderson QC, the UK Independent Reviewer of Terrorism Legislation.

IV. Role of the law in protecting privacy

9 If privacy is to be protected, competing rights and interests have to be balanced in particular cases. Such an exercise can only be carried out through the law, which, at least normally, means legislation setting out the principles and the courts then applying and developing those principles. The law is the watchman on the walls, and there are three overarching problems for the watchman guarding the walls of the citadel of privacy.

10 The first is that the precise extent of the citadel is by no means clear. It is quite hard to define the nature of the right to privacy, not least because it is a relatively new legal right. It has, I think, two main facets: first, the right to prevent anyone from misusing (which can include accessing, retaining, using or disseminating) personal information; and secondly, the right to seclusion, *ie*, the right to personal space, the right to be left alone.[13] But the precise boundary between the private and public spheres is unclear and controversial in many cases.

11 The second overarching problem for the watchman is the difficulty in distinguishing friend from foe. Almost all the rights which privacy rubs up against are rights which, like privacy, are subject to conflicting and strong opinions. Accordingly, a difficult and often potentially controversial balancing exercise has to be carried out, and it is an exercise which requires weighing of factors which are inherently mutually incommensurate.

12 The third overarching problem for the watchman is that, since about 1985, the weaponry available to assault and breach the walls has become remarkably sophisticated and bewilderingly fast-changing, as a result of developments in IT. It is now possible to communicate immediately with almost anybody, indeed with almost everybody, across the globe, and instantly. Further, an enormous amount of personal information is available on the Internet, not merely through our conscious communications, but also through records which we unconsciously make available (*eg*, by shopping online or by using search engines). And all this information is accessible to many entities and people, who may collate it and find it a valuable commodity. Quite apart from this, a huge number of people willingly place large quantities of information about

13 Including freedom from harassment as Tugendhat J explained so well in *Goodwin v News Group Newspapers Ltd* [2011] EMLR 27.

themselves online, without fully appreciating the import of what they are doing.

13 Thus, the Internet, particularly bearing in mind its "almost unlimited search and memory capacity",[14] represents a "quantum leap" in scale over the past. In addition, the Internet is subject to disaggregated control and is effectively outside any single national jurisdiction. Indeed, the whole thrust of the Internet is inconsistent with the core principles of data protection,[15] namely limiting the collection of data to what is strictly necessary for a specific lawful purpose, limiting the use of that data to that purpose, not sharing the data, and deleting the data as soon as it is no longer needed for that purpose.

14 Both statute law, with its prior investigatory, consultative and democratic processes, and the common law, with its focus on gradual development on a case-by-case basis, are therefore facing unprecedented challenges from the Internet, which has been described by one of Google's founders as "the largest experiment in anarchy that we have ever had".[16]

15 These problems for the watchman reinforce the importance of the role of the law in defining the extent of the right to privacy, and indeed the other rights and interests which it rubs up against. Only the rule of law is capable of effectively providing proper protection of such a vital right and defining its limit. This is reflected in the fact that many major human rights instruments require interferences with many rights can only be justified if they are "in accordance with the law".[17]

14 Viviane Reding, Vice-President of the European Commission, *Justice Council: Making Good Progress on Our Justice for Growth Agenda* (26 October 2012).

15 As pointed out in Lee Bygrave, "Data Privacy Law and the Internet: Policy Challenges" in *Emerging Challenges in Privacy Law: Comparative Perspectives* (Normann Witzleb *et al* eds) (Cambridge University Press, 2014) at p 272.

16 Eric Schmidt & Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business* (Knopf, 2013).

17 See, for example, Art 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950; entry into force 3 September 1953); s 1 of the Canadian Charter of Rights and Freedoms, Pt I of the Constitution Act 1982; and s 5 of the New Zealand Bill of Rights Act (1990 No 109). The Singapore Constitution (1985 Rev Ed, 1999 Reprint) also recognises this principle in Arts 9(1) and 14(2) (limitations on the right to life and liberty, and the right to freedom of speech, assembly and association).

V. Current law on privacy and data control

16 By Art 8, the European Convention on Human Rights[18] ("the European Convention"), which dates from 1953, recognises that privacy as a fundamental human right, and, following the enactment of the Human Rights Act 1998[19] ("the 1998 Act"), Art 8 is part of UK law. However, many countries have no law which specifically grants its citizens an express right to privacy. Thus, the constitutions of Singapore and the US do not include a right to privacy; nor do the Charters or Bills of Rights of Canada, New Zealand or Hong Kong.[20] That is scarcely surprising. While the common law has long recognised a right in confidential information, it has been very reluctant to recognise a right to privacy. While the English Court of Appeal refused to recognise a common law right to privacy in 1990,[21] the 1998 Act has changed things and a few months ago it recognised misuse of private information as a tort.[22] The New Zealand courts have been prepared to develop a tort of wrongful publication of private information,[23] and those in Ontario a tort of intrusion on seclusion.[24] And, in an interlocutory judgment last month,[25] the Singapore Court of Appeal has specifically left open the question whether a common law right to privacy should be recognised in this jurisdiction.

17 Apart from the 1998 Act, UK statutes give some protection to privacy, but the pattern of statutory control has rightly been described as being "neither coherent nor comprehensive" so that there is "duplication in some areas and gaps in others".[26] More stringently, Anderson characterised the current state of the principal UK statute governing surveillance for law enforcement and security purposes, the Regulation of Investigatory Powers Act,[27] as "undemocratic, unnecessary and – in the long run – intolerable".[28]

---

18 Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950; entry into force 3 September 1953).

19 c 42 (UK).

20 Canadian Charter of Rights and Freedoms, Pt I of the Constitution Act 1982; New Zealand Bill of Rights Act (1990 No 109); Hong Kong Bill of Rights Ordinance (Cap 383).

21 *Kaye v Robertson* [1990] EWCA Civ 21; [1991] FSR 62.

22 *Google Inc v Vidal-Hall* [2015] 3 WLR 409.

23 *Hosking v Runting* [2005] 1 NZLR 1 at [98]–[99].

24 *Jones v Tsige* [2012] ONCA 32 at [51].

25 *ANB v ANC* [2015] 5 SLR 522 at [20]–[23].

26 Nicole Moreham, "Protection against Intrusion in English Legislation" in *Emerging Challenges in Privacy Law: Comparative Perspectives* (Normann Witzleb *et al* eds) (Cambridge University Press, 2014) at pp 155–156.

27 c 23 (UK).

28 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) Executive Summary at p 8, para 35.

18 Most countries now have legislation which seeks to protect personal data. The Organisation for Economic Co-operation and Development ("OECD") started the ball rolling in 1980,[29] and there was limited national and international action as a result.[30] However, it was only after 1990 that most states really started to appreciate the urgent need for privacy protection in the light of the development of the Internet.[31] This is scarcely surprising: in 1995, only 16 million people used the Internet, whereas now it is over three billion.[32]

19 The European Union ("EU"), with its 29 member states, probably has the highest level of privacy rights and data protection, in the 1995 Data Protection Directive[33] ("the 1995 DPD"), the e-privacy Directive of 2002[34] and the 2006 Data Retention Directive.[35] The Council of Europe (which includes all EU members and around a further 15 European countries) has its own data protection treaty, the so-called Convention 108.[36]

20 The US has relatively weak and patchy legislation protecting data protection.[37] I think that reflects three differences between the US and Europe. First, Europe generally has more faith in regulations whereas the US tends to favour market-based solutions. Secondly, Europe, with its recent history of totalitarian governments, protects

29 Council of the Organisation for Economic Co-operation and Development, *Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980).

30 *Eg*, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS No 108) (28 January 1981; entry into force 1 October 1985).

31 Volker Leib, "ICANN – EU Can't: Internet Governance and Europe's Role in the Formation of the Internet Corporation for Assigned Names and Numbers" (2002) 19 *Telematics and Informatics* 159 at 161.

32 Available at <http://www.internetlivestats.com/internet-users> (accessed November 2015).

33 Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data). See also Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS No 108) (28 January 1981; entry into force 1 October 1985).

34 Directive 2002/58/EC of the European Parliament and of the Council (12 July 2002) (processing of personal data and the protection of privacy in the electronic communications sector).

35 Directive 2006/24/EC of the European Parliament and of the Council (15 March 2006) (retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC).

36 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS No 108) (28 January 1981; entry into force 1 October 1985).

37 See James Whitman, "The Two Western Cultures of Privacy: Dignity *versus* Liberty" (2004) 113 Yale LJ 1151.

privacy rather more than the US, with its commitment to the First Amendment. Thirdly, it is in the US that most IT applications are first developed or implemented,[38] so commercial influence is inevitably greater there than in Europe.

21 Outside Europe and the US, around 60 countries have data protection laws, and research[39] suggests that the European approach has generally been influential.[40] Singapore has the Personal Data Protection Act in 2012,[41] but public authorities are excluded from its ambit, and, while its purpose is not to protect privacy, as a leading commentator has said, it could be invoked for that purpose.[42]

VI. What is private?

22 The difficulties in identifying the boundaries of privacy in the Internet age is well demonstrated by the simple fact that there is still much debate as to what constitutes "personal data", although the legal definition is not particularly controversial; few would quarrel with the definition in Convention 108: "any information relating to an identified or identifiable individual".[43] However, the effect of the definition is not so easy.

23 Thus, so far at least, European courts have been unable to agree whether a person's Internet Protocol address constitutes an item of "personal data".[44] And there is debate as to whether biometric data

38 Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) at pp 107–116.

39 Graham Greenleaf, "Global Data Privacy Laws: 89 Countries and Accelerating" *Privacy Laws & Business International Report* (February 2012); Graham Greenleaf, "The Influence of European Privacy Standards Outside Europe: Implications for Globalisation of Convention 108" (2012) 2 *International Data Privacy Law* 68.

40 Australia enacted data protection legislation in 1988 (Privacy Act (Cth) 1988 ("the 1988 Act")), although initially it only applied to tax file numbers and consumer credit reporting until 2000, and Australia is now considering extending the 1988 Act pursuant to recommendations made in 2008 by its Law Reform Commission. Hong Kong passed a Personal Data (Privacy) Ordinance (Cap 486) in 1995, and Malaysia did so in 2010 (Personal Data Protection Act 2010 (Act 709)) (although it does not cover the public sector).

41 Act 26 of 2012.

42 Simon Chesterman, "After Privacy: The Rise of Facebook, the Fall of Wikileaks and the Future of Data Protection" [2012] Sing JLS 391.

43 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS No 108) (28 January 1981; entry into force 1 October 1985) Annex, Art 1(b), reflecting the Organisation for Economic Co-operation and Development definition: see n 30 above.

44 See the discussion in Lee Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International, 2002) at p 129 *ff*.

counts as personal data.[45] Further, although they are all bound by the same directives, regulations and conventions, different European countries adopt different approaches to anonymising publicly available personal data. For instance, Germany requires anonymisation provided it can be achieved proportionately, whereas Sweden has no such proviso for practicality.[46]

24 More broadly, unlike confidentiality in the context of the law of intellectual property, privacy is a nuanced and multi-faceted concept. In IP law, the position is binary: information loses its confidential status once it is in the public domain, even only to a very limited extent. The position is very different in relation to privacy. The fact that information about an individual is in the public arena does not necessarily prevent that individual from challenging its dissemination more widely, more intensely or more permanently. And privacy also goes further than mere dissemination of information.

25 The nuanced aspect of privacy is vividly demonstrated by the House of Lords decision in *Campbell v MGN Ltd*,[47] where it was permissible to report on a famous model's drug addiction, because she had publicly denied it, but it was impermissible to publish a photograph of her about to enter a rehabilitation clinic, even though she was in a public place: publishing the photograph was too intrusive bearing in mind the public interest in the story. The case involved newspaper coverage, but the same principles apply to the Internet. Indeed, the effect of publication on the Internet is potentially far greater, as in the pre-Internet days most stories in newspapers were relatively limited in distribution (to millions at the most) and quickly forgotten. Nowadays, public actions, events or appearances that are temporary or fleeting and visible to relatively few spectators are subject to distribution to billions of people and to "permanent capture"[48] on the Internet.

26 A telling example of the nuanced nature of privacy on the Internet is the so-called "right to be forgotten". As a "data controller" under the EU 1995 DPD, Google is required to remove data which "appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed". In *Google Spain SL, Google Inc v*

45 See Els Knidt, *Privacy and Data Protection Issues of Biometric Applications* (Springer, 2010) at p 94 *ff*.

46 See, *eg*, *Digital Privacy – PRIME Privacy and Identity Management* (Jan Camenisch *et al* eds) (Springer, 2011) ch 3, at pp 49–50.

47 [2004] 2 AC 457.

48 Moira Paterson, "Surveillance in Public Places: The Regulatory Dilemma" in *Emerging Challenges in Privacy Law: Comparative Perspectives* (Normann Witzleb *et al* eds) (Cambridge University Press, 2014) at p 207.

Agencia Española de Protección de Datos, Mario Costeja González[49] ("*Google Spain*"), a Spanish newspaper had published in 1998 an announcement listing houses which were being sold to recover social security debts from their owners, including Costeja, who were identified. Eleven years later, Google rejected his request to remove the link to this story from their search engine, and the EU court in Luxembourg ("the ECJ") held that they were wrong to do so. As a result, Google and other search engine companies have been prepared to accede to requests to remove outdated, embarrassing stories from their websites.

27 While it is significantly more inclined to favour free speech, it is by no means clear that the right to be forgotten would be automatically rejected in every case in the US. The *Restatement (Second) of Torts*[50] suggests that an action would lie against someone who gives:

> … publicity to a matter concerning the private life of another … if the matter … would be highly offensive to a reasonable person, and … is not of legitimate concern to the public.

This rule is, however, not without its judicial and academic critics and doubters.[51]

28 Some might argue that the right to be forgotten is an example of judges or legislators not recognising reality, given the fact that the story will remain on the Internet, and given also the fact that the increasingly ubiquitous social network services have very limited, if any, control over the activities of end-users, and represent almost limitless powers to search, collect and process information. However, the former Vice-President of the EU Commission, Viviane Reding, recognised this when she described the right to be forgotten as "of course not an absolute right", and she went on to say that it cannot "amount to a right to the total erasure of history" or "take precedence over freedom of expression or freedom of the media".[52]

29 As those observations imply, the need to adopt a realistic approach to the enforcement of privacy and other individual rights on the Internet is of course essential. And that is, I think, recognised by the ECJ in decisions such as *Scarlet Extended SA v Societe Belge des auteurs*[53]

---

49 Case C-131/12 [2014] QB 1022.

50 American Law Institute, *Restatement of the Law Second, Torts* (1977).

51 See, *eg*, George Christie, "The Uneasy and Often Unhelpful Interaction of Tort Law and Constitutional Law in First Amendment Litigation" (2015) 98 Marq L Rev 1003, especially at 1022–1024 and 1029–1030.

52 Viviane Reding, Vice-President of the European Commission, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age* (22 January 2012).

53 Case C-70/10 [2012] ECDR 4.

("*Scarlet Extended*"), where it was held to be disproportionate to expect an Internet Service Provider ("ISP") to monitor systematically for an unlimited period all of its customers' Internet usage to ensure that any block file-sharing did not infringe copyright. The same would apply to infringement of privacy: *Google Spain* only applies where the subject asks for the removal of the link.

VII. Surveillance and law enforcement

30 The need for government surveillance to prevent terrorism and to combat crime is self-evident. Such surveillance is carried out in all sorts of ways – closed-circuit television, satellite monitoring, bugging devices, interception of communications when transmitted or stored, hacking and data sharing. In his 2015 report, David Anderson has said that the relatively low number of deaths of UK nationals from terrorism "owes something to luck … and a great deal to the capabilities of the intelligence agencies and police".[54] And cyber-fraud, bullying, child-grooming and illegal pornography are increasing,[55] much of it on the dark web. All this plainly justifies surveillance by law enforcement agencies and the security services. While electronic communications render electronic surveillance all the more necessary, they also render such surveillance all the more potentially intrusive. The difficult question is how to maximise effective surveillance while minimising any interference with privacy.

31 The UK, like Singapore,[56] Australia[57] and Canada,[58] but unlike the US,[59] does not generally impose a requirement for judicial authorisation before the intelligence services can intercept communications within the jurisdiction. However, the UK has detailed regulations and codes of practice, and, like Canada, the UK has commissioners, who are retired senior judges, to oversee and report on the surveillance activities of the UK law enforcement and security services.[60] The UK also has an Investigatory Powers Tribunal ("IPT") in which anyone can bring proceedings if they believe that their privacy rights have been infringed by government surveillance. The European

54 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) at para 3.14, quoting his previous 2013 report, David Anderson QC, *The Terrorism Acts in 2012* (July 2013).

55 Europol, *The Internet Organised Crime Threat Assessment* (November 2014).

56 Privacy International, *The Right to Privacy in Singapore* (Stakeholder Report, 24th Session, Singapore) (June 2015).

57 Telecommunications (Interception and Access) Act 1979 (Cth).

58 Under the National Defence Act 1985 (RSC, 1985, c N-5).

59 Under the Foreign Intelligence Surveillance Act 50 USC § 1801 *et seq* (1978).

60 These are pretty fully explained in ch 6 of David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015).

Court of Human Rights ("ECtHR") has frequently stated that "in a field where abuse is potentially so easy … and could have such harmful consequences …, it is in principle desirable to entrust supervisory control to a judge",[61] although it accepts that another form of oversight may be acceptable, provided that it was genuinely independent. In a recent decision, currently under appeal, the English High Court held that the UK law on the retention of communications data does not comply with this requirement.[62]

32 The ECtHR in Strasbourg accepts that individual states should be entitled to carry out such surveillance, but insists that it is carried out "in accordance with the law" (*ie*, the power must be contained in clear, appropriate and accessible laws which operate foreseeably),[63] "in pursuit of a legitimate aim", and "proportionate".

33 The Snowden revelations showed that the US intelligence services had been regularly gathering what the US Court of Appeals for the Second Circuit has characterised as "staggering amount of information … on essentially the entire population of the United States" (and much of the rest of the world) "on an ongoing daily basis",[64] and then collating and retaining it in a data bank. The court held that this activity was unlawful as the Patriot Act[65] only permitted the collection and retention of "relevant" information", and this did not entitle the collection of information simply because it might become relevant one day.

34 In a 2006 decision, the ECtHR accepted that the interception of communications by use of catchwords was acceptable,[66] provided its purpose was sufficiently limited and serious (in that case prevention of terrorism), and there were sufficient safeguards and supervision. In a 2009 decision, however, the ECtHR held that the then UK legislation did not give "the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material".[67] A similar criticism was made of the EU's own 2006 Data Retention Directive by the ECJ.[68]

61 *Eg*, *Klass v Germany* (app no 5029/71) at [56].
62 *R (Davis and Watson) v Secretary of State for Defence* [2015] EWHC 1092.
63 *Sunday Times v UK* (app no 6538/74) at [86].
64 *ACLU v Clapper* 785 F 3d 787 (2015).
65 Patriot Act 115 Stat 272 (2001) (US).
66 *Weber v Germany* (app no 54934/00) [2006] ECHR 1173.
67 *Liberty v UK* (app no 58243/00) [2008] ECHR 568 at [69].
68 *Digital Rights Ireland Ltd v Minister of Communications etc* (Joined Cases C-293/12 and C-594/12) [2014] 3 WLR 1607.

35 On two occasions over the past year in the UK, the IPT has ruled that surveillance carried out by the Government Communications Headquarters (responsible for UK's security services' online surveillance) was illegal.

36 In an interesting judgment in 2013,[69] the German Constitutional Court emphasised the differences of approach to data collection and retention for counter-terrorism purposes (prevention) and for policing (detection), and held that the then rules permitting transfer of data from the counter-terrorism database to the police database needed to be significantly more strict and detailed.

VIII. Information obtaining more widely

37 In addition to gathering information to protect national security and to deter and detect crime,[70] governments also obtain much personal data for tax, health and other purposes. And, of course, it is by no means just governments which intrude on privacy. Information is collected about individuals every time they visit a website, shop online, send digital messages and e-mail. And only some of it is knowingly provided; much of it is deduced from various actions or characteristics, as a consequence of cookies, metadata and the like.

38 That information can be used in unexpected ways, especially as it may be passed on to others sometimes in an allegedly anonymised form and sometimes not. For instance, website operators agree to share information they gather with others such as retailers.

39 According to one study, some people may pay more than others when shopping online[71] because of their web browsing history or the make of their mobile phone. And, at least allegedly, online food retailers can tell if a woman is pregnant before her partner, or maybe even she herself, knows it, by identifying changes in her purchasing practices.[72] The Apple watch measures increases in the wearer's heart rate, and it can be linked to what the wearer is looking at on the screen, which can in

69 *Joint Counter-Terrorism Database Case* 1 BvR 1215/07 (24 April 2013).

70 In the UK see the list of permitted interceptions in David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) at paras 6.18 and 6.19.

71 Gerry Smith, "Why Some People Pay More than Others When Shopping Online" *The Huffington Post* (4 November 2014).

72 Kashmir Hill, "How Target Figured out a Teen Girl Was Pregnant before Her Father Did" *Forbes* (16 February 2012).

turn be used to identify appropriate advertising material and other information to be targeted at the wearer.[73]

40 It is also relatively easy to correlate personal information, with ever more sophisticated algorithms and data analysis. As a result, individual pieces of information, seemingly innocuous, in themselves, can be "jigsawed" so as to give a lot more information about us than many of us would be comfortable about. And even when information is anonymised, it is often possible to work out who is being referred to. A leading paper on the topic says it all in its rather off-putting title – "Robust De-anonymization of Large Sparse Datasets".[74]

41 And anyone who has access to data messages can use so-called deep packet inspection ("DPI"), a technique which automatically analyses the contents of data messages sent through the Internet.[75] However, the law may already have conceived of a balancing factor here. If an ISP decided to analyse the content of messages sent through its service through DPI then, although they would gather much more information, it has been suggested with some justification that they may risk losing their status as "mere intermediaries",[76] given the reasoning of the ECJ in the *Scarlet Extended* case.[77]

42 As I have mentioned, the courts have not stood by and allowed national security services to freely invade electronic privacy, and the same is true, albeit perhaps to a significantly more limited extent, when it comes to regulators and the private sector. Google's policy of accumulating information across all its services with the deemed consent of users has been challenged and is apparently viewed by the French Commission nationale de l'informatique et des libertes as breaching the EU Data Protection Directive's information processing standards.[78] And in the US a $22.5m judge-approved fine was negotiated

73 Victoria Woollaston "Tinder Goes Hands-free: Watch App Uses Heart Monitor to Reveal Who Sends Your Pulse Racing" *MailOnline* (7 July 2015) <http://www.dailymail.co.uk/sciencetech/article-3152232/Tinder-goes-hands-free-Watch-app-uses-heart-monitor-reveal-sends-pulse-racing.html> (accessed November 2015).

74 Arvind Narayanan & Vitaly Shmatikov, "Robust De-anonymization of Large Sparse Datasets" in Proceedings of the 2008 IEEE Symposium on Security and Privacy in Oakland, California, US (18–21 May 2008).

75 Milton Mueller *et al*, "Policing the Network: Using DPI for Copyright Enforcement" (2012) 9 *Surveillance & Society* 348.

76 See Chris Marsden, *Net Neutrality: Towards a Co-regulatory Solution* (Bloomsbury Publishing, 2010) at p 72.

77 See n 53 above.

78 Charles Arthur, "Google Privacy Policy Slammed by EU Data Protection Chiefs" *The Guardian* (16 October 2012); France, Commission nationale de l'informatique et des libertes, "Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data across Services" (16 October 2012).

by the Federal Trade Commission in August 2012 with Google for its secret installation of cookies into Apple's Safari browser to enable it to collect private data from Apple users.[79]

IX. Hacking and whistleblowing

43 Quite apart from these relatively lawful activities, there is a real risk of the vast amount of personal information on the Internet not being secure from purely criminal assault.

44 Electronic records are at risk of intrusion on a massive, rapid and sometimes undetectable scale, with electronic "malware", which can wipe, falsify or steal private and sensitive information "with extraordinary thoroughness across a range of networks".[80] Notorious examples include the alleged North Korean swoop on Sony Pictures network, and the very recent raid on and subsequent publication of the Ashley Madison database. And only a few months ago, the US government's personnel management agency reported that hackers, with suspicions centring on China, had stolen from its computer networks sensitive information on over 20 million people who had undergone background checks for security clearances.[81]

45 And there is unlawful leaking (if you disapprove) or whistleblowing (if you approve). Edward Snowden was not the first insider to breach national security; there was Bradley, now Chelsea, Manning responsible for Wikileaks, and Jeffrey Delisle, who provided masses of information to the Russians from US, UK, Canada, Australia and New Zealand intelligence sources. In the UK, the political storm which blew up over Members of Parliament ("MP") expenses in 2009, and still reverberates more than six years later, was precipitated[82] by an inside leak of an electronic record containing every expense claim of every MP.

46 The leaking or theft of hard copy records on these enormous scales would call for an enormous fleet of lorries, or of copying

79 United States, Federal Trade Commission, "Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser" (9 August 2012).

80 Edward Lucas, *Cyberphobia: Identity, Trust, Security and the Internet* (Bloomsbury Publishing, 2015).

81 Patricia Zengerle, "Millions More Americans Hit by Government Personnel Data Hack" *Reuters* (9 July 2015).

82 There had been an earlier request for this information under the UK Freedom of Information Act 2000 (c 36), but it looked as if this would not produce nearly so much, if any, controversial evidence.

machines working for many weeks. By contrast, a single drive the size of a thumb can store more data and 500 million typewritten pages.

47 The way an e-mail is sent provides an easy target for attackers. It is broken up into "packets" of data, which make their way from the sender through different routes to a destination, where they then are reassembled and passed on to the addressee. And even electronic material which is "air-gapped" (*ie*, kept physically separate) can be accessed through a mobile phone adapted to plant spyware on a computer system.[83]

48 And now we have the risk of hacking computer-based, networked drug dispensers, and changing the doses which they are told to administer,[84] or hacking motorcar computers so as to disable the brakes or the power-assisted steering.[85] And there is "ransomware", which is malware which encrypts your documents or other computerised records so that you cannot get access to them, and then you are asked to pay the encrypter a substantial sum to disencrypt.[86] And two weeks ago, there was a reliable report[87] of a blackmailing app which appeared to be a pornographic website but photographed people who logged onto it and then blackmailed them.

49 Systems of data records are not always as well designed as they should be to minimise the risk of inappropriate dissemination. I understand, for instance, that the Australian electronic health record system is an example of the triumph of functionality, in that most parts of it can be accessed by many thousands of health workers without any consideration as to whether such substantial access was required.[88]

X. Self-help methods of protection

50 Our innate sense of risk, which is very well developed in traditional contexts (how to secure one's home or whether it is safe to be

83 Kim Zetter, "Researchers Hack Air-gapped Computer with Simple Cell Phone" *Wired* (27 July 2015) <http://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone> (accessed November 2015).

84 Kim Zetter, "It's Insanely Easy to Hack Hospital Equipment" *Wired* (25 April 2014) <http://www.wired.com/2014/04/hospital-equipment-vulnerable> (accessed November 2015).

85 Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It" *Wired* (21 July 2015) <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway> (accessed November 2015).

86 Alina Simone, "How My Mom Got Hacked" *The New York Times* (4 January 2015).

87 "Porn App Took Secret Photos of Users" *BBC* (7 September 2015).

88 See the Australian Department of Health website <www.ehealth.gov.au>.

out on one's own), has had little opportunity to develop when it comes to the brave new electronic world, which may be why most people do not seem to do much to protect their privacy against lawful or unlawful interception. That is graphically demonstrated by the company UK Gamestation, who, on 1 April 2010, included in their standard online privacy agreement a clause whereby a player agreed that, if he participated in the company's online gaming, the company would permanently own his "immortal soul". Around nine out of ten customers did not notice, and agreed to this.[89]

51 However, it appears that an increasing number of people are using ever-more elaborate technologies to protect their own privacy online. It is no exaggeration to describe the way these various entities interact as a digital arms race. Encryption, which was previously relatively little used by individuals, appears to be increasingly widespread, so much so that the UK government has proposed imposing legal limits on the use of encryption, given that encrypted communications are very difficult (though probably not impossible) to read. This provides a good example of the security arms race, as the proposal has been met by the suggestion of steganography, namely hiding messages in images.[90]

52 In terms of a more coherent development of the law, the EU Commission apparently accepts its present regime is outdated and has proposed a new draft Data Protection Regulation and Directive, which specify rights, such as data portability and the right to be forgotten. And the UK government will very shortly be presenting a new Investigatory Powers Bill for public consultation. As one might expect, in the US, the trend has been more towards encouraging self-help, *eg*, by encouraging Internet companies to make "do not track" options available to customers[91] – mostly with a view to protecting children.

53 The European experience suggests that there is a gap between the regulatory aims and the outcomes. Reports do cast doubt on the effectiveness of enforcement of the 1995 DPD in Europe,[92] and suggest that European data protection agencies are under-resourced, and that

89 Joe Martin, "GameStation: 'We Own Your Soul'" *Bit-Tech* (15 April 2010) <http://www.bit-tech.net/news/gaming/2010/04/15/gamestation-we-own-your-soul> (accessed November 2015).

90 United Nation Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes* (2012) at p 56.

91 *Eg*, Do-Not-Track Online Act of 2011 (S 913, 112th Congress (2011–2012)) and the Act of 2013 (113th Congress (2013–2015)), which were introduced into the Senate by Senator John Rockefeller IV, but neither of which was enacted.

92 *Eg*, European Union Agency for Fundamental Rights, *Data Protection in the European Union: The Role of National Data Protection Authorities* (2010).

compliance with the rules by data controllers is patchy.[93] And if that is the position inside what is probably the most regulated part of the world, what hope is there outside Europe?

XI. International regulation

54 More specifically, the global reach of the Internet means that it cries out for international standards which are uniformly enforced. Unless and until that occurs, local laws have to give such extra-territorial effect as it can. Thus the EU's data protection rules currently apply to a data controller outside the EU, in certain defined circumstances,[94] and it is currently proposed that the new directive should apply to anyone outside the EU who offers goods or services within the EU or monitors behaviour of people within the EU.[95] A fine notion, but it could do with closer definition and there must be question marks over its enforceability.

55 Meanwhile the courts have to do the best they can. The Tribunal de Grande Instance de Paris[96] ordered Yahoo! in the US to block access to anyone with a ".fr" address seeking links to sellers of Nazi memorabilia (the sale of which is illegal in France). Yahoo!'s proceedings in the US complaining of this was rejected by the Court of Appeals for the Ninth Circuit.[97] At least three of the justices held that the US courts had no jurisdiction as the French order only applied to "users located in France". And in Canada three months ago, the British Columbia Court of Appeal was prepared to make a worldwide injunction restraining Google from maintaining links to a site run by a company which was selling goods masquerading as the plaintiff's – passing off.[98] Google was held to have sufficient presence in British Columbia despite having no servers there, because it carried on business there.

---

93 See European Commission, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments: Final Report* (DK/10020, January 2010) and also European Union Agency for Fundamental Rights, *Data Protection in the European Union: The Role of National Data Protection Authorities* (May 2010).

94 Directive 95/46/EC of the European Parliament and of the Council (24 October 1995) (protection of individuals with regard to the processing of personal data and on the free movement of such data) Art 4(1)(c).

95 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation* (COM(2012) 11 final, 25 January 2012) Art 3(2).

96 *LICRA and UEJF v Yahoo! Inc* Mo 00/05309 (2000).

97 *Yahoo Inc v La Ligue Contre le Racisme et Antisemitisme* 433 F 3d 1199 (9th Cir, 2006).

98 *Equustek Solutions Inc v Google Inc* 2015 BCCA 265.

56 There is something of a battle between Google and the EU Commission as to whether Google complies with the right-to-be-forgotten ruling if they delete a record only within the EU, or whether it has to be done worldwide. In this connection, the EU seems to be developing a long-arm jurisdiction which one has tended to associate more with the US.

57 In these circumstances, it is perhaps unsurprising that US business representatives and federal government officials are seeking to water down some of the terms of the EU's proposed Data Protection Regulation.[99] Some may think that it is good that Europe is giving the US a taste of its long-arm medicine, but, more to the point, it highlights the need for international standards.

58 And some steps are being taken in that direction. The Asia-Pacific Economic Cooperation ("APEC") economies have recently established the APEC Cross-border Privacy Enforcement Arrangement to enable national regulators to co-operate and share information in relation to cross-border issues.[100] And under the auspices of OECD, there is an informal network which has the same aim internationally.[101] And, Uruguay signed up to the Council of Europe's Convention 108 two years ago, Morocco is on its way to doing so, Mexico has stated a desire to subscribe,[102] and there is a real prospect of Mauritius and Senegal doing so. Some commentators[103] are optimistic that Convention 108 will receive many further signatories, and may come to represent an internationally accepted set of standards.

XII. Concluding comments

59 When considering the issues thrown up by the Internet, whether in relation to privacy or any other topic, it must be appreciated that we are in a very different world from that which existed 40 years

99 See, *eg*, "US Diplomat Warns of 'Trade War' if 'Right to Be Forgotten' Proposals are Followed Through" *Out-Law.com* (4 February 2013) <http://www.out-law.com/en/articles/2013/february/us-diplomat-warns-of-trade-war-if-right-to-be-forgotten-proposals-are-followed-through> (accessed November 2015).

100 Asia-Pacific Economic Cooperation Cross-border Privacy Enforcement Arrangement (CPEA) <www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-privacy-enforcement-arrangement.aspx> (accessed November 2015).

101 Global Privacy Enforcement Network, "About the Network" <www.privacyenforcement.net>.

102 Cristos Velasco, "Mexico Expressed Interest in Adhering to the Council of Europe's Convention 108" *Protección Datos México* (2 April 2012).

103 See Jörg Polakiewicz, "Convention 108 As a Global Privacy Standard?" International Data Protection Conference, Budapest (17 June 2011).

ago. Whether we are making, developing, interpreting or implementing laws and rules relating to privacy in this new world, we would do well to remember what the Chinese philosopher King Wu-ling said more than 2,000 years ago, namely that "a talent for following the ways if yesterday is not sufficient to improve the world of today".[104]

60 However, we must also remember that we are dealing with fundamental values, and should not assume that our concerns about the threats to privacy from modern technology are as exceptional as they seem. One hundred and twenty-five years ago, a future US Supreme Court judge, Louis Brandeis, and another prominent lawyer, Samuel Warren, wrote of "[r]ecent inventions and business methods" which "call[ed] attention" to the fact that:[105]

> … photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten … that what is whispered in the closet shall be proclaimed on the house tops.

61 In the light of the all-pervasive, fast-developing and anarchic nature of the Internet, it is at times tempting to accept the pithy observation made by one of the founders of Sun-Microsystems, namely: "You have zero privacy. Get over it."[106] But that is not the way to go. The State has a duty to protect its citizens against the excesses of the State itself as well as the invasions of rights by others. People care about their privacy, even if they often do little to protect it. And with its substantial potential for criminality – hacking, cyber-fraud, illegal pornography, grooming and bullying – as well as for defamation and other civil wrongs, electronic communication systems have to be subject to a degree of regulation and control.

62 The aim must be to identify a suite of regimes which is practical and, as far as possible, enables us to obtain all the benefits of the Internet with minimum reduction in privacy, and which also has public confidence. People must have confidence that their personal data is not inappropriately accessed, and in so far as it is accessed by governments (whether for surveillance purposes or otherwise) or by commercial entities – or indeed by anyone else – that it will not be misused. To achieve that, there must be clear regulations, with clear standards, conditions and safeguards, and proper enforcement, supervision and

104 King Wu-ling 307 BC: Nicola di Cosmo, *Ancient China and its Enemies: The Rise of Nomadic Power* (Cambridge University Press, 2002) at p 137.

105 Louis Brandeis & Samuel Warren, "The Right to Privacy" (1890) 4 Harv L Rev 193.

106 Polly Sprenger, "Sun on Privacy: Get over It" *Wired* (26 January 1999) <www.wired.com/political/law/news/1999/01/17538> (accessed November 2015); Jacob Morgan, "Privacy is Completely and Utterly Dead, and We Killed It" *Forbes* (19 August 2014).

liability regimes, governing the obtaining, using, storing, sharing, dissemination and destruction of such data. And ideally, these should be on a common international basis and to a common international standard, at least when it comes to commercial organisations.

63 When it comes to making the rules, the law makers and regulators must not just talk to other law makers and regulators. They must also talk to the developers of the technology and designers of systems, in order to decide what is practically feasible, and to identify the potential risks, particularly so far a security is concerned. All this is easy to say, but the devil is in the detail.

64 When it comes to commercial entities obtaining personal data, we have to bear in mind that the data is often used for the benefit of the individual concerned, notwithstanding that it is also for the benefit of the commercial entity. We have to decide whether, and to what extent, we want to, and are practically able to, limit the rights of website-owners as to the use and sharing of information which they obtain from us. We need to decide the extent to which the right to be forgotten should be extended, and whether we can give clearer guidance on when information about a third party which is in the public domain or a fleeting nature should not be published more widely and permanently.

65 There is an increasing risk that public availability of anonymised data can lead to identification of individuals, but it cannot be right to outlaw the collation of such data or access to it: the benefits to health and welfare from the existence and availability of such data are well known. Various ways of ensuring anonymity have been mooted, including differential privacy,[107] secure multiparty computation[108] and homomorphic encryption,[109] but they are still work in progress. If any of these solutions does the trick, then it should be required to be in place in relation to any available anonymised datasets.

66 Turning to surveillance, the so-called "war on terror" throws up particularly difficult issues for legislators and for the courts. Quite apart from highlighting the acute conflict between respect for privacy and the need for surveillance, it is a war which has no legal status, no clear end and no fully defined enemy. The cases which I have mentioned seem to suggest that, at least so far in relation to this war, the courts are not simply giving in to the executive's wishes, and are adhering to the rule of

107 Or indistinguishability – see <https://en.wikipedia.org/wiki/Differential_privacy> (accessed November 2015).

108 <https://en.wikipedia.org/wiki/Secure_multi-party_computation> (accessed November 2015).

109 <https://en.wikipedia.org/wiki/Homomorphic_encryption> (accessed November 2015).

law – in contrast to the Second World War where the US Supreme Court upheld an executive order consigning all Japanese Americans into internment,[110] and the House of Lords effectively permitted the Government to imprison a person for no good reason.[111] While I have no doubt but that this should continue, judges should be aware that they are treading a very delicate line.

67 Particularly when it comes to surveillance, it has fairly been said[112] that judicial involvement is important in order to ensure public confidence, especially following the Snowden revelations. In particular, there is obviously much to be said for requiring prior judicial permission in every case, as in the US. However, *ex parte* applications which will never go *inter partes* have their drawbacks. So there is also much to be said for the UK system of commissioners investigating *ex post facto* provided that they are free to make full subsequent investigations. In an ideal world, one would, I suppose, have both. And it must be right to spell out matters such as the criteria which are to be applied when considering whether to permit different sorts of surveillance, and deciding what can and cannot be done with personal data once obtained. While international standards for surveillance may also be desirable, they are self-evidently harder to achieve.

68 When it comes to unlawful assaults on private data, on the other hand, international co-operation, in terms of both standards and enforcement, is both desirable and, I would have thought, largely achievable, On a more practical level, designers of systems must not always favour, or be encouraged to favour, functionality over security. And there is much to be said for the view that manufacturers and suppliers should ensure, as far as possible, that their products can be patched (preferably remotely) to fix any security holes which may be discovered after sale. Further, manufacturers and suppliers should be required to own up to problems rather than to hide them, as has happened on occasion.[113]

69 Indeed, more openness is highly desirable more generally, as it normally is. However, one has to accept that it can only go so far. The security services and law enforcement agencies require a degree of

110 *Korematsu v United States* 323 US 214 (1944).

111 *Liversidge v Anderson* [1942] AC 206.

112 *Eg*, David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015).

113 See, *eg*, Lisa O'Carroll, "Car Hacking Scientists Agree to Delay Paper That Could Unlock Porsches" *The Guardian* (30 July 2013) and Jamie Grierson, "Security Flaw Affecting More Than 100 Car Models Exposed by Scientists" *The Guardian* (18 August 2015).

secrecy, but it is encouraging to note that, in his recent report,[114] Anderson calls for more openness from the UK government when it comes to surveillance on UK terrorism legislation.

70 During this talk, I have made much of the point that the far-reaching developments in IT require that steps are to taken to ensure that the right to privacy is appropriately protected. However, we must also bear in mind the possibility, indeed the likelihood, that the relationship between developments in technology and the right to privacy is not a one-way street. It is, I suggest, inevitable that the developments in IT that we are witnessing will change our attitude to privacy, and that is essentially for two reasons. First, one only has to consider the way that IT has changed the patterns and character of all aspects of our lives to appreciate that it is very likely to affect our values as well. Secondly, the existence of the Internet inevitably affects what can be practically achieved in terms of enforcement of privacy, and the law should never seek to acknowledge or enforce rights which are in practice unenforceable.

71 In what way and to what extent our attitude to privacy will be affected is a matter of speculation, but I strongly suspect that, as is the normal way of things, perplexing and uncertain as future developments may seem today, they will appear to have been obvious with wisdom of hindsight. And while this is a factor which makes the watchman's difficult task even harder, it is also one which makes it much more interesting.

---

114 David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) at para 13.3(a).