Singapore Academy of Law Annual Lecture 2015

Is nothing secret? Confidentiality, Privacy, Freedom of Information and Whistleblowing in the Internet Age[1]

Lord Neuberger

21 September 2015

Preface

1. It is a signal honour to be invited to give this lecture, especially in Singapore's fiftieth 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, "holds 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"[2].

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[3] what we called "an impressively wide-ranging judgment"[4] given by your Chief Justice[5] 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 had built up in the UK through merely advertising its services meant

[1] 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* (ed N Witzleb, D Lindsay, M Paterson and S Rodrick, 2014), as well as to D Anderson QC for his June 2015 Report, *A Question of Trust: Report of the Investigatory Powers Review*

[2] The quotes are taken from *The Economist Supplement on Singapore*, 18 July 2015, *passim*

[3] *Starbucks (HK) Ltd v British Sky Broadcasting Group PLC* [2015] UKSC 31, [2015] 1 WLR 2628

[4] *Ibid*, paras 45 and 66

[5] *Staywell Hospitality Group Pty Ltd v Starwood Hotels & Resorts Worldwide Inc* [2013] SGCA 65, [2014] 1 SLR 911

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 "*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*"[6].

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 IP right, although it has only relatively recently been recognised by the law. Today, most international conventions on human rights and liberties now protect the right to privacy.[7] And, in March this year, the UNHRC in Geneva created a new UN Special Rapporteur on "the Right to Privacy in the Digital Age".[8]

4. As Sir Zelman Cowan famously said forty-five years ago, "*A man without privacy is a man without dignity*"[9]. 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 prison where all the prisoners could be under observation at any point. He described it as "*a new*

---

[6] *Starbucks supra*, para 63

[7] Universal Declaration of Human Rights Article 12; United Nations Convention on Migrant Workers Article 14; UN Convention of the Protection of the Child Article 16; International Covenant on Civil and Political Rights Article 17. Provisions in regional conventions include: Article 10 of the African Charter on the Rights and Welfare of the Child; Article 11 of the American Convention on Human Rights; Article 4 of the African Union Principles on Freedom of Expression; Article 5 of the American Declaration of the Rights and Duties of Man; Article 21 of the Arab Charter on Human Rights; and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality. (this list is taken from the Privacy International website: https://www.privacyinternational.org/)

[8] Press Release, 26 March 2015: http://www.ohchr.org/

[9] Z. 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".

mode of obtaining power of mind over mind, in a quantity hitherto without example"[10]. And the 20th century French philosopher, Michel Foucault suggested that "*a state of conscious and permanent visibility that assures the automatic functioning of power*" and "*should tend to render its actual exercise unnecessary*"[11].

5. However, even the identity and nature of fundamental rights may vary with time and place. As I recently pointed out[12], 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[13]. And the recent, very different, public reactions in Germany and France to the proposed grant of statutory powers of electronic interception to national security services highlights the territorial variations. A wide-ranging new law in France, with is 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[14], has caused much outrage[15]. The attitude in the UK appears to be somewhere in the middle, whereas in the USA the public has only become generally concerned about government surveillance since the revelations made by Julian Assange and Edward Snowden.[16] However, in the past seventy years, we have been developing international norms in some areas of human rights which it is now reasonable to treat as universal.

Privacy is a qualified right

6. Even though it is generally regarded as an important legal right, privacy is not an absolute right: it has to be subject to constraints. Perhaps the most frequently encountered constraint is when

[10] J Bentham, *The Works of Jeremy Bentham*, vol. 4 (1843), p 39
[11] M Foucault, *Discipline and Punish* trans. Alan Sheridan , p.201
[12] https://www.supremecourt.uk/docs/speech-150512.pdf, paras 2-7
[13] Although privacy was recognised in some ancient texts as pointed out by D Anderson in his *Review op cit* (fn 1) para 2.3
[14] http://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers.
[15] http://www.wsj.com/news/articles/SB10001424052702303874504579372832399168684?mg=reno64-wsj.
[16] see D Anderson *op cit* (fn 1), paras 2.26-2.33

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. But that does not alter the fact that in deciding whether to permit a newspaper to publish a story about someone, the law is balancing two conflicting rights against each other.

7. 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 more balanced and thoughtful analysis of the tension between national security and privacy can be found in the report[17] published a couple of months ago by David Anderson QC, the UK Independent Reviewer of Terrorism Legislation.

The role of the law in protecting privacy

8. If privacy is to be protected, competing rights and interests have to be balanced in particular cases. In broad terms, that exercise involves policing the boundaries between the public and the private, the individual and other individuals, the individual and the state. Such an exercise can only properly be carried out through the law, which, at least normally, means legislation which sets out the principles and the courts which then apply and develop those principles. The law is the watchman

[17] *op cit* (fn 1)

on the walls is in point, and there are three overarching problems for the watchman guarding the citadel of privacy.

9. The first is that the precise extent of the citadel protected by the walls 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 two main conceptual dimensions. First, the right to prevent anyone from misusing (which can include accessing, retaining, using or disseminating) personal information. Secondly, the right to seclusion, ie the right to personal space, the right to be left alone[18]. But the precise boundary between the private and public spheres is unclear and controversial in many cases.

10. The second overarching problem for the watchman is the difficulty in distinguishing friend from foe. Almost all the rights which privacy rubs up against rights, are, like privacy, often 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.

11. 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 communications technology. It is now possible to communicate immediately with almost anybody, indeed with almost everybody, across the globe. Further, an enormous amount of information is available about all of us on the internet, not merely through our intended, voluntary communications, but also through information which we are required to provide (eg to hospitals or when we apply for a licence) or which we unconsciously

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

make available (eg by shopping on line 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. In addition, huge numbers of people willingly place large quantities of information about themselves online, without fully appreciating the import of what they are doing.

12. Thus, the internet, particularly bearing in mind its "almost unlimited search and memory capacity"[19], represents what many would call a "quantum leap"[20] in scale over the past. In addition, the internet is subject to disaggregated control and is effectively outside any single national jurisdiction. Indeed, that the whole thrust of the internet is inconsistent with the core principles of data protection[21], 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.

13. And it is not just the internet. CCTV enables peoples' public locations to be identified, and a mobile phone enables its owner's movements to be monitored, as do tracking devices and GPS. It is relatively easy now to record mobile phone conversation in the street via a listening device close to the speaker. Secret photography or filming is easy with mobile phones. And face-recognition technology coupled with remote filming enables almost random invasion of privacy. And fresh developments are occurring all the time.

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

[19] Viviane Reding http://europa.eu/rapid/press-release_SPEECH-12-764_en.htm
[20] An inappropriate expression when one thinks about it; in nuclear physics, a quantum leap is almost the smallest change one could imagine
[21] As pointed out in L Bygrave *Data privacy Law and the Internet* in *Emerging Challenges in Privacy Law* (ed Witzleb et al, 2014) p 272

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*"[22], and which is subject to frequent significant developments.

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 limits. 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*"[23].

The current law on privacy and data control

16. By article 8, the European Convention on Human Rights (the European Convention), which came into effect in 1953, recognises that privacy as a fundamental human right, and, following the enactment of the Human Rights Act 1998 (the 1998 Act), article 8 is part of UK law. However, even now, not every democratic country has a law which grants its citizens an express right to privacy. Thus, the constitutions of Singapore and the United States do not include a right to privacy; nor do the Charters or Bills of Rights of Canada, New Zealand or Hong Kong[24]. 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. The English Court of Appeal refused to recognise a common law right to privacy in 1990[25], but the 1998 Act has changed things and a few

[22] E Schmidt and J Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business* (2013)
[23] See for example, Article 8 ECHR, section 1 of the Canadian Charter of Rights, and section 5 of the New Zealand Bill of rights. And the Singapore Constitution recognises this principle in articles 9(1) and 14(2) (limitations on the right to life and liberty, and the right to freedom of speech, assembly and association).
[24] Canadian Charter of Rights and Freedoms 1982, New Zealand Bill of Rights 1990, Hong Kong Bill of Rights Ordnance cap 383
[25] *Kaye v Robertson* [1990] EWCA Civ 21, [1991] FSR 62

months ago the court recognised misuse of private information – which covers most, if not all, aspects of privacy - as a tort[26]. And, in an interlocutory judgment last month[27], the Singapore Court of Appeal has specifically left open the question whether a common law right to privacy should be recognised in this jurisdiction. The Australian federal government's attempts to introduce a statutory cause of action for breach of privacy have been abandoned, or at least postponed, as a result of ferocious criticism from the newspapers.

17. Apart from the 1998 Act, UK statutes give some protection to privacy - eg by restricting interception of electronic messages, while seeking to maintain national security[28], protection from harassment[29] and stalking[30], and criminalising revenge porn, whereby rejected lovers place compromising photos of the rejecting party on the internet, was made a criminal action this year, carrying a maximum sentence of two years[31]. The various UK statutes which afford protection differ in their approach and extent, and 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*"[32]. More stringently, Mr Anderson characterised the current state of the principal UK statute governing surveillance for law enforcement and security purposes, RIPA, as "*undemocratic, unnecessary and – in the long run- intolerable*".[33]

---

[26] *Google Inc v Vidal-Hall* [2015] 3 WLR 409
[27] *ANB v ANC* [2015] SGCA 43, paras 20-23
[28] Relevant legislation includes Regulation of Investigatory Powers Act 2000, Terrorism Act 2000, Wireless and Telegraphy Act 2006, sections 48-49 and Data Retention and Regulatory Powers Act 2014
[29] Protection from Harassment Acts 1997, sections 2 and 4
[30] Ibid, sections 2A and 4A – added by Protection of Freedoms Act 2012
[31] Criminal Justice and Courts Act 2015, sections 33-35
[32] N Moreham, *Protection against intrusion in English legislation* in *Emerging Challenges in Privacy Law* (eds Witzleb and ors, 2014), pp 155-156
[33] D Anderson in his *Review op cit* (fn 1), Executive Summary, p 8, para 35

18. Most countries now have legislation which seeks to protect personal data. The OECD started the ball rolling in 1980[34], and there was limited national and international action as a result[35]. 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[36]. This is scarcely surprising: in 1995, only 16 million people used the internet, whereas now it is over 3 billion[37].

19. The EU, with its 29 member states, probably has the highest level of privacy rights and data protection, in the 1995 Data Protection Directive, the 1995 DPD[38], which was followed by the e-privacy Directive of 2002[39], and the 2006 Data Retention Directive[40]. The Council of Europe (which includes all EU members and a further 15 European countries) has its own data protection Convention, Convention 108[41], and a 2001 protocol ensures that it now closely aligned with the EU's 1995 DPD.

20. The US has relatively weak and patchy legislation protecting data protection[42]. 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 privacy rather more than the US, with its commitment to the

---

[34] Council of the OECD, *Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal data*, 23 Sept 1980
[35] Eg the Council of Europe's *Convention 108* – see below
[36] V Leib *ICANN – EU Can't: Internet Governance and Europe's Role* …. (2002) 19 Telematics and Informatics 159, 161
[37] *http://www.internetlivestats.com/internet-users/*
[38] Directive 95/46/EC , [1995] OJ L 281, and see Convention 108
[39] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector
[40] Directive 2006/24/EC on the 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
[41] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981
[42] See J Whitman, *the Two Western Cultures of Privacy: Dignity versus Liberty* (2004) 113 Yale Law Journal 1151; and, since this lecture was given, the point has been emphasised by the Opinion of the Advocate general in *Schrems v Data Protection Commissioner* – see footnotes 91 and 115 below.

First Amendment. Thirdly, it is in the US that most IT applications are first developed or implemented[43], so commercial concerns are inevitably greater there than in Europe.

21. Outside Europe and the US, around sixty countries have data protection laws, and research[44] suggests that the European approach has generally been influential[45]. Singapore passed the Personal Data Protection Act in 2012, 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[46].

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". The expression itself is relatively uncontroversially defined in Convention 108[47], which itself followed the OECD guidance[48], as "any information relating to an identified or identifiable individual". So far at least, European courts have been unable to agree whether a person's IP address constitutes an item of "personal data"[49]. And there is debate as to whether biometric data counts as personal data[50]. Further, although they are all bound by the same directives, regulations and conventions, different European countries adopt different approaches to anonymising publicly available

---

[43] L Bygrave *Data Privacy Law: An International Perspective* (2014), pp 107-116
[44] G Greenleaf, *Global Data Privacy Laws: 89 Countries and Accelerating* (2012) and *The Influence of European Privacy Standards Outside Europe: Implications for Globalisation of Convention 108* (2012) 2 International Data Privacy Law 68
[45] Australia enacted data protection legislation in 1988[45], 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 Data Protection Ordinance in 1995, and Malaysia did so in 2010 (although it does not cover the public sector).
[46] S Chesterman, *After Privacy: the Rise of Facebook, the Fall of Wikileaks and the Future of Data Protection* [2012] Singapore Journal of Legal studies 391
[47] Article 1(b) of the Annex to Convention 108
[48] see fn 34
[49] See the discussion in L Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (2002), pp 129ff
[50] See E Knidt *Privacy abd data Protection Issues if Biometric Applications* (2010) pp 94ff

personal data. For instance, Germany requires anonymisation provided it can be achieved proportionately, whereas Sweden has no such proviso for proportionality[51].

23. 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 normally 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, as already discussed, privacy also goes further than mere dissemination of information, and importantly includes the right to be left alone.

24. It is as unrealistic to say that if one does not wish to have ones privacy interfered with one should not go online as it is to say that if well-known individuals didn't want candidly taken photos to be widely published, they should not leave their houses. In that connection, the nuanced nature of privacy is vividly demonstrated by the House of Lords *Campbell* decision[52], where it was held to be permissible to report on a famous model's drug addiction, but only because she had publicly denied it, while it was held to be impermissible to publish a photograph of her about to enter a rehabilitation clinic, even though she was in a public place. The case involved newspaper coverage, but the same principles apply to the internet. Indeed, the effect of publication on the internet is greater because public actions, events or appearances that are fleeting and visible to relatively few spectators are now not merely subject to publication in newspapers which would be seen by at

[51] See eg *Digital Privacy – PRIME Privacy and Identity Management*, ed J Camenisch et al, Chap 3, pp 49-50
[52] *Campbell v MGN Ltd* [2004] 2 AC 457

most a few million people and are thrown away next day, but are now subject to "permanent capture"[53] and global distribution to billions of people on the internet.

25. 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[54], 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 the *Google Spain* case[55], a Spanish newspaper had published in 1998 an announcement listing houses which were being sold to recover social security debts from their owners, including Mr 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.

26. Earlier this year, the Netherlands courts refused to order Google to remove links to a TV broadcast showing a "hitman", who had been convicted a number of years ago, discussing a projected attack with his client. As it did not name the man, merely his alias, and the crime in question was serious, the court refused him any relief[56]. And "[t]he right to be forgotten has arrived in Japan", according to Professor Hiroshi Miyashita of Chuo University, Tokyo as a result of a court in Tokyo ordering Google to remove the removal of links to sites suggesting the plaintiff was guilty of criminal activities[57].

---

[53] M Paterson *Surveillance in Public Places* in *Emerging Challenges* … (op cit) p 207
[54] European Data Protection Directive (Directive 95/46EC)
[55] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González,* case C-131/12
[56] *X v Google Netherlands BV* ECL:NL:GHAMS:2015:1123
[57] Gruber *Global Constitutionalism 2015*, p V-12

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 USA. Section 652D of the *Restatement (Second) of Torts*[58] 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[59].

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*"[60].

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 the *Scarlet Extended* case[61], where it was held to be disproportionate to expect an Internet Service Provider to monitor systematically for an unlimited period all of its customers' internet usage to ensure that any block file-sharing did not infringe copyright. I see no

---

[58] 1977

[59] See eg G Christie *The Uneasy and Often Unhelpful Interaction of Tort Law and Constitutional Law in First Amendment Litigation,* (2015) 98 Marquette LR 1003, especially at pp1022-1024 and 1029-1030

[60] V Reding, 22 January 2012, http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

[61] *Scarlet Extended SA v Societe Belge des auteurs* (Case C-70/10) [2012] ECDR 4

reason why the same would not apply to infringement of privacy: *Google Spain* only applies where the subject asks for the removal of the link.

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 – CCTV, 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"[62]. And cyber-fraud, bullying child-grooming and illegal pornography are increasing[63], much of it on the dark web. All this plainly justifies surveillance by law enforcement agencies and the security services. However, 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 minimise the consequential interference with privacy.

31. The UK, like Singapore[64], Australia[65] and Canada[66], but unlike the US[67], does not generally impose a requirement for prior judicial authorisation to conduct surveillance. However, the UK has detailed regulations and codes of practice, and provides for retired senior judges to oversee and report on the surveillance activities of the UK law enforcement and security services[68], The UK

[62] D Anderson in his Review op cit (fn 1), para 3.14 quoting his previous 2013 report *The Terrorism Acts in 2012*
[63] Europol, *The Internet Organised Crime Threat Assessment*, (November 2014).
[64] https://www.privacyinternational.org/sites/default/files/Singapore_UPR_PI_submission_FINAL.pdf
[65] Telecommunications (interception and Access) Act 1979
[66] Under the National Defence Act 1985
[67] Under the Foreign Intelligence Surveillance Act 1978
[68] These are pretty fully explained in chapter 6 of David Anderson's report *op cit*, fn 1

also has an Investigatory Powers Tribunal, IPT, in which anyone can bring proceedings of they feel that their privacy rights have been infringed by government surveillance.

32. David Anderson recommends a requirement of prior judicial approval (as well as a widening of the ambit of the commissioners' role)[69]. The ECtHR has made clear its view 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*"[70], 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[71].

33. The European Court of Human Rights in Strasbourg (the ECtHR) 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)[72], and that it is "in pursuit of a legitimate aim" and "proportionate".

34. 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*"[73], and then collating and retaining it in a data bank. The Court held this activity was unlawful as the Patriot Act only permitted the collection and retention of "relevant" information", and this did not entitle the collection of information simply because it might become

[69] D Anderson in his *Review op cit* (fn 1), recommendation 22
[70] Eg *Klass v Germany* (app no 5029/71), para 56
[71] R *(Davis and Watson) v Secretary of State for Defence* [2015] EWHC 1092 (Admin)
[72] *Sunday Times v UK* (app no 6538/74), para 86
[73] *ACLU v Clapper* 785 F.3d 787 (May 7, 2015)

relevant one day. (The decision revealed that an investigator identifies a "seed" suspicious phone number, from which calls would then be looked at, and that the investigator then moved on to numbers called from that phone, "first hops", and then to numbers called from the first hops, "second hops" etc. President Obama reduced the number of permitted hops from three to two, and required a Judge to approve the identification for a seed number.)

35. In a 2006 decision, the ECtHR accepted that the interception of communications by use of catchwords was acceptable[74], 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 "*the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material*"[75]. A similar criticism was made of the EU's own 2005 Data Retention Directive by the European Court of Justice[76]. The Directive was defective as it did not exclude material which was privileged or irrelevant, gave no guidance as to what constituted serious crime, contained no clear limitations on access to and use of data, and had no provision for judicial review before the data was accessed.

36. On two occasions over the past year in the UK, the IPT has ruled that surveillance carried out by GCHQ (responsible for UK's security services' online surveillance) was illegal. In one case, the IPT held that information received from the US government had not, at least initially, been obtained "in accordance with the law", and concern was expressed about safeguards which were in place.[77] In the other, the intercepted material (which GCHQ was ordered to destroy) was held to be protected by legal privilege.[78]

---

[74] *Weber v Germany* (app no 54934/00) [2006] ECHR 1173
[75] *Liberty v UK* (app no 58243/00) [2008] ECHR 568, para 69
[76] *Digital Rights Ireland Ltd v Minister of Communications etc*, Joined Cases C-293/12 and C-594/12 [2014] 3 WLR 1607
[77] *Liberty v Secretary of State* [2015] UKIPTrib 13_77-H
[78] *Belhadj v Security Service* [2015] UKIPTrib 13_132-H

37. In an interesting judgment in 2013[79], 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.

Information obtaining more widely

38. In addition to gathering information to protect national security and to deter and detect crime[80], 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 email. 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.

39. 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.

40. According to one study, some people may pay more than others when shopping online[81] because of their web browsing history or the make of their mobile phone. And, at least allegedly, on-line food retailers can tell if a woman is pregnant before she knows it herself by identifying changes in

[79] *Joint Counter-Terrorism Database Case* 1 BvR 1215/07 (24 April 2013)
[80] In the UK see the list of permitted interceptions in D Anderson *op cit*, (fn 1), paras 6.18 and 6.19
[81] http://www.huffingtonpost.com/2014/11/04/pay-more-shopping-online_n_6099698.html

her purchasing practices[82]. The Apple watch measures increases in the wearer's heart rate, which can then be linked to what the wearer is looking at on the screen, which in turn can then be used to identify appropriate advertising material and other information which can then be targeted at the wearer[83].

41. It is also relatively easy to correlate various items of data from different sources, with the assistance of 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: for instance, by linking the anonymised Massachusetts Group Insurance Commission database (which recorded each patient's birthday sex and ZIP code) with voter registration records, a researcher identified the medical record of the Governor of Massachusetts[84]. A leading paper on the topic says it all in its rather off-putting title - *Robust De-anonymisation of Large Sparse Datasets*[85].

42. 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[86]. 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

---

[82] http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

[83] http://www. dailymail.co.uk/sciencetech/article-3152232/Tinder-goes-hands-free-Watch-app-uses-heart-monitor-reveal-sends-pulse-racing.html

[84] C Dwork and A Roth *The Algorithmic Foundations of Differential Privacy* , Foundations and Trends in Theoretical Computer Science. Vol. 9, nos 3–4, p 206, Aug. 2014

[85] A Narayanan and V Shmatikov *Robust De-anonymisation of Large Sparse Datasets* in *SP 08 and SP 09 Proceedings of IEEE Symposia on Security and Privacy* (2008 and 2009)

[86] M Mueller et al, *Policing the Network: Using DPI for Copyright Enforcement* (2012)

losing their status as "mere intermediaries"[87], given the reasoning of the ECJ in the *Scarlet Extended* case[88].

43. As I have mentioned, the courts have not stood by and allowed national security services freely to 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 (CNIL) as breaching the EU Data Protection Directive's information processing standards[89]. And in the US a $22.5m Judge-approved fine was negotiated by the FTC 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[90]. And there is currently a challenge, which has (since I gave this talk) been held to be a potentially valid challenge by the ECJ, to the European Commission's ruling that personal data can be transferred from the EU to the USA.[91]

Hacking and whistleblowing

[87] See C Marsden *Net Neutrality: Towards a Co-Regulatory Solution* (2010), p 72
[88] See fn 32 above
[89] http://www.theguardian.com/technology/2012/oct/16/google-privacy-policies-eu-data-protection, and http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-incomplete-information-and-uncontrolled-combination-of-data-across-ser/
[90] https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented
[91] Two days after this lecture was delivered, Advocate General Bot published his opinion holding that the ruling was indeed invalid in *Schrems v Data Protection Commissioner* – ECLI:EU:C:2015:627, and since then the ECJ has given its decision, agreeing with that opinion – see para 58 and fn 115 below. The decision is on-line at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

44. Quite apart from the (mostly lawful) activities I have been discussing, there is the unappetising fact that there is a big question mark over the question whether most of the vast amount of personal information on the internet is secure from purely criminal assault.

45. 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"[92]. 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[93].

46. And there are unlawful leaks (if you disapprove) or (if you approve) plucky whistleblowing. 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 enormous political storm which blew up over MPs' expenses in 2009, and still reverberates more than six years later, was precipitated[94] by an inside leak of an electronic record containing every expense claim of every MP.

---

[92] E Lucas, *Cyberphobia: Identity, Trust, Security and the Internet* (2012) Preface, p2

[93] http://www.reuters.com/article/2015/07/09/us-cybersecurity-usa-idUSKCN0PJ2M420150709

[94] There had been an earlier request for this information under the Freedom of Information Act 2000, but it looked as if this would not produce nearly so much, if any, controversial evidence

47. The reproduction of hard copy records on the enormous scales of these leaks would call for an enormous fleet of lorries, or of copying machines working for many weeks. By contrast, a single drive the size of a thumb can store more electronic data than 500 million typewritten pages.

48. The way an email is sent also 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. 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[95].

49. And now we have the risk of hacking computer-based, networked drug dispensers, and changing the doses which they are told to administer[96], or hacking motorcar computers so as to disable the brakes or the power-assisted steering[97]. 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[98]. And two weeks ago, there was a reliable report of a blackmailing app which appeared to be a pornographic website but photographed people who logged onto it and then blackmailed them.

50. Systems of data records are not always as well designed as they could be, and therefore should be, in orde 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

[95] http://www.wired.com/2015/07/researchers-hack-air-gapped-computer-simple-cell-phone/
[96] http://www.wired.com/2014/04/hospital-equipment-vulnerable/
[97] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[98] http://www.gvsu.edu/e-hr/ransomware-121.htm?gclid=CIeSs-vB5McCFUZAGwod8vECBg

most parts of it can be accessed by many thousands of health workers without any consideration as to whether such substantial access was required[99].

Self-help methods of protection

51. Our sense of risk, which is very well-developed in familiar traditional contexts (how to secure one's home or whether it is safe to be 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 company UK Gamestation, who, on 1 April 2010, included in their standard on-line privacy agreement a clause whereby a punter agreed that, if he participated in the company's on-line gaming, the company would permanently own his "*immortal soul*". Around nine out of ten customers did not notice, and agreed to this[100].

52. However, it appears that an increasing number of people are using ever-more elaborate technologies to protect their own privacy online. For example, TOR[101] on the dark net aims to make online activity very difficult to associate with an individual; and VPNs[102] operate as proxy servers masking the identity of the sender of an email. 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

[99] See www.ehealth.gov.au and www0.health.nsw.gov.au/pubs/2008/healthlink_summary.html
[100] J Martin www.bit-tech.net/news/gaming/2010/04/15/gamestation-we-own-your-soul
[101] https://en.wikipedia.org/wiki/Tor_(anonymity_network). Origin: The Onion Rooter
[102] Virtual Private Networks

example of the security arms race, as the proposal has been met by the suggestion of steganography, namely hiding messages in images[103].

53. 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[104], 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 USA, the trend has been more towards encouraging self-help, eg by encouraging internet companies to make "do not track" options available to customers[105] - mostly with a view to protecting children.

54. The European experience suggests that there is a gap between the regulatory aims and the outcomes. The European Commission recognised more than ten years ago that the "*'data explosion' inevitably raises the question whether legislation can cope with [the] challenges*" to privacy rights thrown up by the internet[106]. Subsequent reports cast doubt on the effectiveness of enforcement of the 1995 DPD in Europe[107], and suggest that European data protection agencies are under-resourced, and that compliance with the rules by data controllers is patchy[108]. And if that is the position inside what is probably the most regulated part of the world, what hope is there elsewhere?

---

[103] United Nation Office on Drugs and Crime, *the Use of the Internet for Terrorist Purposes* (2012), p 56.
[104] See fn 68
[105] 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
[106] European Commission, *First report on the Implementation of the Data protection Directive* (2003)
[107] Eg EU Agency for Fundamental Rights, *Data Protection in the European Union: the Role of National Data Protection Authorities* (2010)
[108] See http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf and also EU Agency for Fundamental Rights, *Data Protection in the European Union: the Role of National Data Protection Authorities*, both 2010 reports

International Regulation

55. 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 circumstance[109], 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[110]. A fine notion, but it could do with closer definition and there must be question marks over its enforceability.

56. Meanwhile the courts have to do the best they can. The Tribunal de Grande Instance de Paris[111] 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[112]. 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[113]. Google was held to have sufficient presence in British Columbia despite having no servers there, because it carried on business there.

---

[109] Article 4(1)(c)
[110] EU proposal, article 3(2)
[111] *LICRA and UEJF v Yahoo! Inc* Mo 00/05309 (2000)
[112] *Yahoo Inc v La Ligue Contre le Racisme et Antisemitisme* 433 F.3d 1199
[113] *Equustek Solutions Inc v Google Inc* 2015 BCCA 265

57. 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 world-wide. In this connection, the EU seems to be developing a long-arm jurisdiction which one has tended to associate more with the United States.

58. 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[114]. Some may think that it is good that Europe is giving the United States a taste of its long-arm medicine, but, more to the point, it highlights the need for international standards. The need for international co-operation was highlighted two days after this talk was delivered by Advocate General Bot's Opinion in the ECJ case C-362/14 *Schrems v Data Protection Commissioner*, where he concluded that the US laws protecting personal data were at least arguably inadequate by EU standards, and accordingly, contrary to what was stated in the DPD, it was open to a national courts (in that case the Irish courts) to rule that data gathered within the EU could not be transferred to the USA. Two weeks later this Opinion was effectively followed by the ECJ[115]. Whatever decision the Irish court reaches, the need for international standards and co-operation in this field has, I suggest, been given strong support by the Opinion and, even more, by the judgment.

59. And some steps are being taken in that direction. The Asia-Pacific Economic Cooperation economies have recently established the APRC Cross-Border Privacy Enforcement Arrangement to enable national regulators to cooperate and share information in relation to cross-border

[114] See eg http://www.out-law.com/en/articles/2013/february/us-diplomat-warns-of-trade-war-if-right-to-be-forgotten-proposals-are-followed-through/
[115] See footnote 91 above

issues[116]. And under the auspices of OECD, there is an informal network which has the same aim internationally[117]. 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[118], and there is a real prospect of Mauritius and Senegal doing so. Some commentators[119] are optimistic that Convention 108 will receive many further signatories, and may come to represent an internationally accepted set of standards.

Concluding comments

60. 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 of years 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 2300 years ago, namely that "*a talent for following the ways if yesterday is not sufficient to improve the world of today*"[120].

61. However, we must also remember that we are dealing with fundamental values, and we should not assume that our concerns about the threats to privacy from modern technology are as exceptional as they seem. As long as 125 years ago, a future US Supreme Court Judge, Louis Brandeis and a prominent legal academic, Samuel Warren, wrote of "*[r]ecent inventions and business methods*" which

---

[116] *APEC 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
[117] Global Privacy Enforcement Network, *About the Network* www.privacyenforcement.net
[118] http://protecciondatos.mx/2012/04/esmxico-muestra-inters-en-adherirse-al-convenio-108-del-consejo-de-europaenmexico-expressed-interest-adhering-council-europes-convention-108/?lang=en
[119] See J Polakiewicz on http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD_documents/Convention_108as_a_global_privacy_standards_June_2011.pdf
[120] King Wu-ling 307 BC: N di Cosmo, *Ancient China and its Enemies: the Rise of Nomadic Power* (2002) p 137

"*call[ed] attention*" to the fact that "*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*"[121].

62. It is at times tempting to accept the pithy observation made by one of the founders of Sun-Microsystems, who said that the effect of the internet is that "*You have zero privacy. Get over it*"[122]. 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.

63. 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. If people are to have confidence that personal data accessible by governments (whether for surveillance purposes or otherwise) or commercial entities will not be misused, there must be clear regulations, with clear standards, conditions and safeguards, and proper enforcement, supervision and 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. Particularly considering that it is now 20 years old, those responsible for drafting the EU's 1995 DPD did a pretty good job, both in terms of style and content, but things have moved on in the ensuing twenty years.

---

[121] L Brandeis and S Warren, *The Right to Privacy* (1890) 4 Harvard LR 193

[122] S McNeally, *Sun on Privacy: Get Over It*, 26.1.99 www.wired.com/political/law/news/1999/01/17538. And J Morgan, Forbes.com 19.08. 2014: *Privacy is completely and utterly dead, and we killed it.*

64. 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 as security is concerned.

65. As to commercial entities obtaining and using 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 user. We have to decide whether, and to what extent, we want to limit, and are practically able to limit, the ability of website-owners to retain, use and share of information which they obtain in various ways. We need to decide the extent, if any, 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 public to an extent or temporary cannot be published more widely and permanently.

66. The fact that there is an increasing risk that public availability of anonymised data can lead to identification of individuals, cannot jutify outlawing 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[123], secure multiparty computation[124], and homomorphic encryption[125], but they are still works in progress. If any of these systems works, then it should be required to be in place in relation to any available anonymised datasets.

[123] Or instinguishability – see https://en.wikipedia.org/wiki/Differential_privacy
[124] https://en.wikipedia.org/wiki/Secure_multi-party_computation
[125] https://en.wikipedia.org/wiki/Homomorphic_encryption

67. Turning to surveillance, the 'War on Terror' throws up particularly difficult issues for legislators and for the courts. Striking the right balance between the executive's wishes and individual's fundamental rights in such a context is a fraught business, and a number of similar examples from the Second World War era indicate how difficult such an exercise can be. While upholding the rule of law should plainly continue, judges should be aware that they are treading a very delicate line.

68. Particularly when it comes to surveillance, it has fairly been said[126] 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.

69. So far as unlawful assaults on personal data are concerned, 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 to favour, or be encouraged to favour, functionality over security. And there is much to be said for the view that 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,

[126] Eg D Anderson

manufacturers and suppliers should be required to own up to problems rather than to hide them, as has happened on occasion[127].

70. 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 secrecy, but it is encouraging to note that, in his recent report[128], Mr Anderson calls for more openness from the UK government when it comes to surveillance on UK terrorism legislation.

71. As usual, openness is vital; there has been something of a cult of secrecy as to what governments are doing to monitor people's electronic communications - and their activities more widely by electronic means, and as to what data the private sector is collecting, retaining, collating, and sharing. Obviously, openness can only go so far. The security services and law enforcement agencies require a degree of secrecy, but I draw support from the fact that Mr Anderson calls for more openness in his recent report[129] on UK Terrorism legislation.

72. 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 IT and fundamental rights is not a one-way street. It is, I suggest, inevitable that developments in technology 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

---

[127] See eg http://www.theguardian.com/technology/2013/jul/30/car-hacking-ignition-injunction and http://www.theguardian.com/technology/2015/aug/18/security-flaw-100-car-models-exposed-scientists-volkswagen-suppressed-paper

[128] D Anderson in his *Review op cit* (fn 1), para 13.3(a)

[129] D Anderson in his *Review op cit* (fn 1), para 13.3(a)

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.

73. 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.

74. As common lawyers, we are steeped in the notion that the law is not merely based on principle, and that practicality is just as important. That tradition should stand us in good stead when we face up to dealing with the problems I have been discussing this evening.

75. Finally, a post script apology to my Latin teachers. As is apparent from various passages in this talk, I have decided to throw in the towel in the fight to maintain the etymologically unchallengeable contention that "data" is a plural word. There is a point at which correctness becomes pedantic obstinacy.

David Neuberger Singapore, 21 September 2015