Freedom from Suspicion

Surveillance Reform for a Digital Age

a JUSTICE report

Freedom from Suspicion

Surveillance Reform for a Digital Age

October 2011

JUSTICE – 50 years of defending the rule of law

JUSTICE is an independent law reform and human rights organisation. It works largely through policy-orientated research; interventions in court proceedings; education and training; briefings, lobbying and policy advice. It is the British section of the International Commission of Jurists (ICJ).

JUSTICE relies heavily on the help of its members and supporters for the funds to carry out its work. For more information visit www.justice.org.uk.

JUSTICE, 59 Carter Lane, London EC4V 5AQ
020 7329 5100
admin@justice.org.uk
www.justice.org.uk

ISBN: 978-0-907247-53-1
Designed by Adkins Design
Printed by Hobbs the Printers

Contents

Executive summary

- In 2000, Parliament enacted RIPA. At the time, it was acclaimed by government ministers as human rights-compliant, forward-looking legislation.

- Since RIPA came into force in 2000, there have been:
  - more than 20,000 warrants for the interception of phone calls, emails, and Internet use;
  - at least 2.7 million requests for communications data, including phone bills and location data;
  - more than 4,000 authorisations for intrusive surveillance, eg, planting bugs in someone's house or car;
  - at least 30,000 authorisations for directed surveillance, eg, following someone's movements in public, or watching their house.

- In total, there have been close to three million decisions taken by public bodies under RIPA in the last decade.

- This does not even begin to include the number of warrants and authorisations on behalf of MI5, MI6 and GCHQ, which have never been made public.

- Of the decisions we do know about, fewer than 5,000 (about 0.16 per cent) were approved by a judge.

- The main complaints body under RIPA, the Investigatory Powers Tribunal, has dealt with only 1,100 cases in the last decade.

- In the last decade, it has upheld only ten complaints.

- Surveillance is a necessary activity in the fight against serious crime. It is a vital part of our national security. It has saved countless lives and helped convict hundreds of thousands of criminals.

- Unnecessary and excessive surveillance, however, destroys our privacy and blights our freedoms.

- RIPA has not only failed to check a great deal of plainly excessive surveillance by public bodies over the last decade but, in many cases, inadvertently encouraged it. Its poor drafting has allowed councils to snoop, phone hacking to flourish, privileged conversations to be illegally recorded, and CCTV to spread. It is also badly out of date.

- RIPA is neither forward-looking nor human rights compliant. Piecemeal amendments are no longer enough for what is already a piecemeal Act. Root-and-branch reform of the law on surveillance is needed to provide freedom from unreasonable suspicion, and put in place truly effective safeguards against the abuse of what are necessary powers.

- This report, therefore, outlines a series of recommendations to serve as the basis for a draft Surveillance Reform Bill.

Acknowledgements

Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists.

JUSTICE would like to thank the Joseph Rowntree Charitable Trust for its funding of this project.

We would also like to thank the following for their helpful discussions and sharing of information concerning surveillance and the Regulation of Investigatory Powers Act: Professor Ben Goold, Dr Shane Mac Giollabhui, Dr Chris Pounder, Professor Charles Raab and John Wadham. The law relating to the Investigatory Powers Tribunal (IPT) was addressed in two of JUSTICE's recent interventions before the UK Supreme Court – R(A) v B in 2009 and Tariq v Home Office in 2011 – and we are grateful to counsel who acted pro bono for us in those cases: Lord Pannick QC and Tom Hickman in R(A) v B and John Howell QC and Naina Patel in Tariq. Please note, however, that the views expressed in this report, responsibility for any mistakes, and the analysis and conclusions drawn, are those of JUSTICE alone.

This report was written by Eric Metcalfe, JUSTICE's director of human rights policy. It was researched by JUSTICE policy interns Mevlüde Akay, Laura Giles, Portia Harris, Matshidiso Mohajane, Sangeetha Iengar, Nina Ross and Rachel Shepherd.

Chapter 1
Introduction

1. English law has for centuries been fiercely protective of privacy as a fundamental value. As Sir Thomas Erskine May wrote in his *Constitutional History of England* in 1863:[1]

> Next in importance to personal freedom is *immunity from suspicions and jealous observation*. Men may be without restraints upon their liberty; they may pass to and fro at pleasure; but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators – who shall say that they are free? Nothing is more revolting to Englishmen than the espionage which forms part of the administrative system of continental despotisms. It haunts men like an evil genius, chills their gaiety, restrains their wit, casts a shadow over their friendships, and blights their domestic hearth. *The freedom of this country may be measured by its immunity from this baleful agency*.

2. More than four decades ago, JUSTICE published a report in which we warned that the right to privacy was increasingly under threat from recent, rapid advances in technology:[2]

> Privacy has been infringed as long as man has lived in society; in every community, there have always been eavesdroppers, gossips and peeping Toms. But until very recent times, the physical means of infringement available to these have been our natural senses, apparatus with which we are all familiar and against which we know instinctively how to protect ourselves. The arrival of advanced electronics, microcircuits, high-definition optics, infra-red film and the laser beam have changed all this. *The ordinary man today can no longer ascertain by ordinary means whether or not he is being watched or overheard…*

Our report found that the common law was no longer adequate to protect individual privacy on the basis that we had 'already achieved technical possibilities which were never contemplated by the common law and against which the private individual cannot effectively defend himself'.[3] We

1. *Constitutional History of England 1760-1860*, Vol II (1863), 287-288. Emphasis added. For a detailed discussion of the right to privacy under the common law see Chapter 2 below.
2. *Privacy and the* Law (JUSTICE, 1970), para 110. Emphasis added.
3. Ibid, para 116. In an appendix to the report, we highlighted a number of potential technological developments that would likely involve further threats to privacy, including the growth of ATMs, government and commercial databases, CCTV cameras and even the eventual rise of the Internet – see eg, appendix E, para 7: 'Where, only ten years ago, personal information on individuals was scattered throughout the country in small units held on pieces of paper in manilla folders (and, therefore, for all practical purposes impossible to bring together in one place), much of this information has by now found its way into the storage systems of different computers. *At the present time, these have not yet begun to talk to each other. But just as the railways and the telegraphs began with a number of independent lines and, by the inexorable pressures of economics were ultimately welded together into nation-wide systems, so it is only a matter of time before the computers, with their attendant storage systems, become interconnected into a single network'*.

concluded that 'English law is seriously defective as it now stands, and there is an urgent need for legislation'.[4]

3. At the time that we made these recommendations in 1970, mobile phones and DNA profiling had not yet been invented. The Internet was barely more than a dozen mainframe computers in the US,[5] whose existence was entirely unknown to the public at large. There were no CCTV cameras in town centres in the UK[6] and the number of cameras on the London Underground could be counted on one hand.[7]

4. In 2011, our prediction that the pace of technological change would continue to outstrip the law's ability to protect privacy has proved all too accurate. For example:

   - There are now somewhere between 1.8 million to 4.2 million surveillance cameras in the UK.[8] Even using the lowest estimate, this means that there are more cameras per capita in the UK than in any other country in the world. In 2009, for instance, the BBC reported that the London borough of Wandsworth operates more than a thousand cameras, more than the cities of Boston, Dublin and Johannesburg combined.[9] The Shetland Islands alone has more than one hundred CCTV cameras, more than the city of San Francisco with a population of more than 800,000.[10]

   - Nor is surveillance limited to ground-based cameras. In February 2010, for instance, Merseyside Police used an aerial surveillance drone equipped with thermal imaging cameras to track a stolen car,[11] and police are now seeking permission to operate aerial surveillance drones in a number of force areas, including metropolitan London in advance of the 2012 Olympics.[12]

   - There are approximately 80 million active mobile phone subscriptions in the UK.[13] As a Royal Academy of Engineering report explained in 2007, 'as long as it is switched on, a person's mobile phone can reveal where they are, within a range of 150-400 metres in urban areas'.[14] In addition, each voice or data call made with a mobile phone produces data that includes the details of the subscriber (including name, billing address, and the method of payment used, such as bank details), their location, the length of the call or the amount of data

4. Ibid, para 10.
5. In 1969, ARPANET had four working nodes. By 1971, this had grown to 15 nodes in 23 locations, all of which were either universities, research institutes or defence facilities.
6. See 'CCTV in Britain: Working Paper No 3' by McCahill and Norris, *Urban Eye*, March 2002, para 2.1.
7. *CCTV Today*, November 1996. Five black-and-white cameras were installed in Holborn Station in 1961 but CCTV was not installed elsewhere on the Underground until the mid-1970s.
8. The overall number of CCTV cameras in the UK continues to be a subject of considerable debate. The estimate of 4.2 million cameras was derived from an academic survey of CCTV in Putney in 2002 (see McCahill and Norris, 'CCTV in London: Working Paper No 6' by McCahill and Norris, *Urban Eye*, June 2002), while a more recent survey carried out by police community support officers in Cheshire on behalf of ACPO was used to support an estimate of 1.8 million cameras: see eg, 'CCTV camera estimates halved by police', BBC News, 3 March 2011.
9. 'The statistics of CCTV', BBC Newsnight, 20 July 2009. The statistics were based on Freedom of Information requests made by the BBC of more than 100 local authorities in the UK.
10. Ibid.
11. 'Eye in the sky arrest could land police in the dock', the *Guardian,* 15 February 2010.
12. See eg, 'CCTV in the sky: police plan to use military-style spy drones', by Paul Lewis, the *Guardian,* 23 January 2010 detailing plans to establish the use of UAVs by a number of agencies including the UK Border Agency and HM Revenue and Customs.
13. Ofcom, *The Communications Market 2010*, fig 5.47 on p322 showing 80.3 mobile phone connections in 2009. An active mobile phone subscription is one that has been used within the last 90 days.
14. Royal Academy of Engineering, *Dilemmas of Privacy: Challenges of Technological Change* (March 2007), para 6.2.1.

downloaded, as well as the manufacturer, model and serial number of the mobile phone itself.

- More than 60 per cent of people in the UK use the Internet on a daily basis, whether via a desktop computer, a laptop or – increasingly – a mobile phone.[15] According to the latest figures,[16] 82.2 per cent of the UK population has used the Internet at least once, with the figure rising to 98.7 per cent of those aged between 16 and 24. As with mobile phone usage, each Internet session generates a substantial amount of data that is stored across the Internet in a number of different locations. Data about someone's visit to websites such as Google, Facebook, YouTube, Twitter and eBay, for instance, will be stored not only by those sites but also by the relevant Internet Service Provider ('ISP') on the person's computer or phone, as well as on the various routers and servers used to transfer the information.

- The UK's surveillance camera network includes a system of Automatic Number Plate Recognition ('ANPR') operated by both public bodies and private companies which records the time, date and location of about 15 million vehicles each day.[17] Each vehicle sighting (or 'read') is currently stored at the police's National ANPR Data Centre for a minimum of five years.

- The National DNA Database (NDNAD) holds the DNA profiles of about five million people,[18] making it the world's largest DNA database, both per capita and in absolute terms.[19] Approximately one million of these profiles belong to people who have never been charged with or convicted of a criminal offence.[20] Although the database records only DNA profiles, rather than samples, a tissue sample must always be taken in order to generate a profile. A single sample of DNA contains some of the most intimate medical information about another human being that it is possible to gather. Almost all of the profiles on the NDNAD have been developed from samples that were taken without the person's consent.[21] The use of DNA technology in crime detection is not limited to the police. Since 2003, for instance, more than 11,000 portable DNA saliva kits have been issued to staff on the Underground and London buses.[22]

- Most people in the UK carry a number of cards in their wallet or purse which contain not only magnetic strips but also microchips and, increasingly, radio-frequency identification (RFID), enabling them to gather large amounts of information concerning a person's finances, movements and habits. Credit and debit cards alone are used to make more than 23 million transactions in the UK each day,[23] and details of each transaction are stored electronically.

---

15. According to an Office for National Statistics press release dated 27 August 2010, 60% of the UK population access the Internet daily, double the figure recorded in 2006.
16. Office for National Statistics, *Internet Access Quarterly Update*, 18 May 2011.
17. National Policing Improvement Agency website, visited June 2011. The ANPR network was introduced by the Metropolitan Police in 1997, following an earlier initiative by the City of London Police. It was subsequently extended to more than 23 force areas in 2004.
18. House of Commons Home Affairs Committee, *The National DNA Database* (HC 222, March 2010), para 13.
19. There are several biometric databases in other countries that are larger, eg, the iris-scan database in the United Arab Emirates, but the NDNAD is the world's largest DNA database.
20. Home Affairs Committee report, n18 above, para 13.
21. As of 31 March 2011, there were 43,886 samples retained on the NDNAD from volunteers, out of a total of 6.6 million samples (source: National Policing Improvement Agency website; visited 14 June 2011). Note that the total number of samples is greater than the estimated number of persons whose profile is recorded on the NDNAD. This is because a number of samples are thought to be duplicates or recorded under a different name (see Home Affairs Committee report, n18 above, p 7).
22. See eg, 'Tube Staff get DNA testing kits', the *Daily Telegraph,* 15 August 2003; 'Driver's spit kit traps bus assault', the *Times,* 27 October 2004; 'DNA kits issued to all London bus drivers', Transport for London press release, 23 May 2008.
23. UK Cards Association, *Quarterly Statistical Release,* 3 December 2010.

In addition, store loyalty cards such as the Tesco Clubcard may gather considerable amounts of information, not only about a customer's grocery shopping but also, increasingly, a broad range of services including travel, broadband, car insurance, banking, and mobile phone contracts. Similarly, the Oyster Card operated by London Transport contains an RFID chip that allows the full journey and transaction history of each individual cardholder on London Transport services to be stored.

5. As these examples demonstrate, the UK has, in the space of 40 years, gone from a society in which mass surveillance was largely a theoretical possibility to one in which it has, in a variety of shapes and forms, become not only ubiquitous but also routine, viral and even airborne. We do not doubt that many of these changes have brought enormous benefits (see eg, the Internet). Nor is the ability to track a stolen car or identify a suspect from a DNA sample something to be slighted. But the ever-increasing capacity of others to gather so much information about our daily lives undoubtedly comes at a severe cost to our privacy.

6. Fortunately, the law has not stood still since our 1970 report. We recommended, for instance, the adoption of data protection legislation to regulate 'those modern computerised data banks which purvey personal information',[24] and the first Data Protection Act was passed in 1984. The European Communities Act 1972, enacted following the UK's entry into the European Union (EU), set the stage for a number of important privacy-enhancing measures to be directly effective in British courts (along with several unwelcome privacy-diminishing ones). We also campaigned for the UK's obligations under the European Convention on Human Rights (ECHR) to be incorporated into domestic law and in 1998 Parliament enacted the Human Rights Act (HRA), which, among other things, imposed a duty on government ministers and public bodies to act compatibly with Convention rights, including the right to respect for private and family life under Article 8.

7. However, the general provisions of Article 8 ECHR were never intended to be a substitute for proper regulation of the use of surveillance and in 1998 we published *Under Surveillance: Covert policing and human rights standards*, which was strongly critical of the existing piecemeal scheme of regulation. Among other things, we argued for a comprehensive legal framework to govern the use of surveillance powers by police and other public bodies, with prior judicial authorisation for any measure that seriously interfered with privacy rights.[25]

8. In response to criticisms such as these, Parliament enacted the Regulation of Investigatory Powers Act 2000 (or 'RIPA' as it is more commonly known).[26] Introducing the Bill, the then-Home Secretary Jack Straw MP waxed effusive:[27]

---

24. *Privacy and the Law*, n2 above, para 135: 'quite apart from any general remedy for infringement of privacy it may be necessary to control by special legislation those modern computerised data banks which purvey personal information. What appears to be required is a method of ensuring that the information they hold is accurate, that it is accessible only to those who are lawfully authorised to extract it, and that the individual to whom it relates can check it, correct it where necessary, and discover to whom it has been given'.
25. See eg, Recommendation 1: 'Existing legislation covering the use of technical surveillance devices – the Interception of Communications Act 1985 and the Police Act 1997 – should be reviewed with the aim of providing a single regulatory system for the interception by law enforcement agencies of all forms of communication (including email). The system should be based on a coherent set of principles as required by Art 8 of the European Convention. There should be no exemption from the statutory controls for operations where one party has consented to the surveillance ('participant monitoring')'.
26. Shortly after RIPA was passed, the Scottish Parliament also enacted the Regulation of Investigatory Powers (Scotland) Act 2000, which contains similar provisions to that of the Westminster Parliament.
27. Hansard, HC Debates col 767, 6 March 2000.

This is an important Bill, and represents a significant step forward for the protection of human rights in this country. Human rights considerations have dominated its drafting.

Indeed, RIPA was widely heralded as a new and proportionate framework for the use of surveillance powers, and the government made much of its promise that the new laws would be compatible with rights under the HRA and the ECHR.

9. In truth, however, RIPA was never the model legislation that the government promised. Poorly drafted and hopelessly opaque, it was not so much a comprehensive framework for surveillance powers so much as a crude stitching-together of different regulatory regimes that were each highly complex in their own right and, taken together, lacked all coherence. For example, the same mobile phone conversation between two terrorist suspects may be admissible or inadmissible as evidence in criminal proceedings depending on the means by which it was recorded (eg, whether the call was picked up by a hidden microphone or intercepted respectively). The same activity of planting a surveillance device in someone's house may be authorised by a politician or by a judge depending entirely on whether the agency responsible is an intelligence body (eg, MI5) or a law enforcement one (eg, the police). And the commissioner responsible for ex post facto oversight of these kinds of surveillance activity will correspondingly differ according to the means used – the Interception of Communications Commissioner for interceptions, the Surveillance Commissioner for intrusive surveillance by law enforcement, or the Intelligence Services Commissioner for intrusive surveillance by the intelligence agencies. With many key surveillance powers subject to authorisation by the executive rather than a judge, and with insufficient oversight of the executive's exercise of those powers, this is a legislative scheme that no reasonable person would describe as ideal.

10. More generally, RIPA contains little or nothing to regulate some of the most obvious forms of surveillance in our society. For example, despite millions of surveillance cameras in the UK, there is nothing in RIPA that deals explicitly with the regulation of CCTV or ANPR. It should come as little surprise, therefore, to learn that the past decade has witnessed an unprecedented expansion in surveillance which RIPA has done little to check and much to facilitate. For example:

- More than 20,000 interception warrants have been issued in the UK since RIPA came into force a decade ago[28] - more than in the previous two decades put together.[29] A single warrant can cover either all the communications (phone, email, post, etc) of a single person, or all the communications from a single premises.[30] A warrant generally lasts three months but may be renewed.[31]

- In addition to the issue of more than 20,000 interception warrants, there have been an untold number of interceptions carried out by authorities without a warrant, including routine interceptions carried out by the Prison Service.[32]

---

28. A total of 20,054 warrants were issued by the Home Secretary and the Scottish Executive between 2000-2010 (source: annual reports of the Interception of Communications Commissioner from 2000-2010.) The number of interception warrants issued by the Foreign Secretary or the Minister for Northern Ireland remains unknown.
29. A total of 12,799 warrants were issued by the Home Secretary and the Secretary of State for Scotland between 1990-1999 and a total of 4,641 warrants were issued by the Home Secretary and the Secretary of State for Scotland between 1980-1989 (source: Statewatch, *UK Surveillance Statistics 1937-2010,* www.statewatch.org/uk-tel-tap-reports.htm).
30. Section 8(1).
31. Section 9(6)(c).
32. See section 4 of RIPA prescribing the various circumstances in which an interception warrant is not necessary.

- In January 2011, the Metropolitan Police announced that it would undertake a fresh investigation of allegations of phone hacking by reporters working for the *News of the World* tabloid, following revelations that it had failed to contact large numbers of possible victims in the course of its earlier investigations in 2005-2006.[33] In the course of ongoing parliamentary inquiries, it emerged that the Metropolitan Police had previously and for several years carried out its investigations on the basis that secretly accessing another person's voicemail did not constitute a criminal offence under section 1 of RIPA (unlawful interception of communications) if the other person had already listened to the voicemail.[34] This raises the possibility that an unknown number of unwarranted interceptions may have been carried out by the police and other public bodies during this period in the belief that a warrant was not required.

- Between September and October 2006, BT secretly intercepted and profiled the Internet sessions of 18,000 of its customers as part of a trial of an Internet advertising platform created by the US company Phorm.[35] The trial of the platform, originally known as PageSense but later called Webwise, involved monitoring the online activity of customers without their knowledge or consent for the purposes of delivering web-based advertisements targeted at individual users. Details of the secret trial were revealed by the media in 2008, leading to a large number of complaints against BT and Phorm. Although the City of London Police, the Information Commissioner's Office and the Crown Prosecution all declined to take any action against BT or Phorm,[36] the complaints were taken up by the European Commission which launched infringement action against the UK government in April 2009, alleging among other things that the provisions of RIPA failed to provide sufficient protection against unlawful interception of communications, contrary to EU law. In September 2010, the Commission referred the UK government to the Court of Justice of the European Union concerning its continuing failure to amend RIPA.[37]

- Since 2005, there have been more than 2.7 million requests by police and other public bodies for the communications data belonging to private individuals, including more than 3,000 requests by local authorities.[38] Between July 2009 and December 2010 alone, Google received more than 3,670 requests from UK government agencies for data concerning individual users.[39]

---

33. See eg, *Bryant and others v Metropolitan Police Commissioner* [2011] EWHC 1314 (Admin) at para 12 per Foskett J: 'Although not revealed publicly until 2010, some 4 or 5 years later, following requests under the Freedom of Information Act, it seems that Mr Mulcaire was in possession of 91 unique PIN codes and related mobile telephone numbers, as well as other information about individuals and that the overall material found in Mr Mulcaire's and Mr Goodman's possession contained 4,332 names or partial names and 2,978 numbers or partial numbers for mobile phones, along with 30 audio tapes containing recordings of voicemail messages'. In July 2011, Sue Akers, the Metropolitan Police's Deputy Assistant Commissioner in charge of the reopened investigation, told the House of Commons Home Affairs Select Committee that approximately 3,870 individuals had been identified so far, along with roughly 5,000 landline numbers and 4,000 mobile phone numbers (House of Commons Home Affairs Committee, *Unauthorised tapping into or hacking of mobile communications* (HC 907, 20 July 2011), para 89).
34. See eg, the report of the House of Commons Home Affairs Committee, *Unauthorised tapping into or hacking of mobile communications* (HC 907, 20 July 2011), paras 27-35. See also the evidence of Assistant Commissioner John Yates to the House of Commons Committee on Culture Media and Sport on 2 September 2009 and 28 March 2011, and to the House of Commons Home Affairs Committee on 7 September 2010 and 29 March 2011.
35. See eg, 'BT and Phorm secretly tracked 18,000 customers in 2006', by Chris Williams, the *Register,* 1 April 2008; 'BT admits tracking 18,000 users with Phorm system in 2006' by Charles Arthur, the *Guardian,* 3 April 2008.
36. See e.g. 'CPS decides no prosecution of BT and Phorm for alleged interception of browsing data', CPS press statement, 8 April 2011; 'Watchdog rules out punishment over Phorm trials', ZD Net, 9 June 2008; 'Police drop investigation into BT's Phorm trials', ZD Net, 23 September 2008.
37. See e.g. 'Commission refers UK to court over privacy and personal data protection', EU Commission press statement, 30 September 2010 (IP/10/1215).
38. See Chapter 4 below.
39. See www.google.com/transparencyreport/governmentrequests/GB/

- Between 2002 and 2010, there have been 172,353 law enforcement authorisations for directed surveillance by law enforcement bodies.[40] Between 2003 and 2010, there have been a further 59,840 authorisations for directed surveillance by non-law enforcement bodies (including government departments and local authorities).[41]

- In February and March 2008, Poole Borough Council conducted covert surveillance of a family of five, following suspicion that the parents had given a false address on an application for one of their children to attend the local school. The RIPA authorisation was granted by the council's head of legal services and included permission to observe 'the day to day movements of the family' by 'use of a digital camera to record images of persons entering and/or exiting both addresses'.[42] The surveillance lasted three weeks and involved the Council education officer driving past two properties owned by the family to see whether they were being used, parking nearby in order to watch who was getting in or out of the family car, and on one occasion following the mother on a school run.[43] Despite a widespread public outcry, the Chief Surveillance Commissioner Sir Christopher Rose declared that 'media criticism of Poole Borough Council was misplaced'.[44] In July 2010, though, the IPT ruled that the Council's authorisation to carry out surveillance of the family had been unnecessary and disproportionate, and thus contrary to Article 8 ECHR.[45] However, the Tribunal refused to rule out that using surveillance operations for the sake of investigating possibly dishonest applications for school places was generally outside the scope of RIPA.[46]

- Between 2000 and 2010, there have been 4,096 authorisations for intrusive surveillance by law enforcement bodies;[47] and more than 24,790 authorisations for property interference, including 1,699 residences, 378 offices and 403 hotel bedrooms.[48]

- In March 2006, the Prime Minister Tony Blair confirmed that the assurance given by Harold Wilson to Parliament in 1966 that 'there was to be no tapping of the telephones of Members of Parliament' – known as the Wilson Doctrine[49] – remained in force,[50] despite advice from the then-Interception of Communications Commissioner Sir Swinton Thomas.[51] In February 2007, Sir Swinton made public his criticisms in his annual report, describing the exemption for MPs from interception as 'a striking illogicality' that 'flies in the face of our Constitution and is wrong'.[52] In February 2008, it emerged that private conversations between Sadiq Khan MP and Babar Ahmad, a constituent who was an inmate at Woodhill Prison, had been covertly recorded at the direction of the Metropolitan Police Counter-Terrorism Division during two visits that Mr Khan made to the prison in May 2005 and June 2006.[53] This led to a number of complaints that this had breached the spirit, if not the precise terms, of

40. See Chapter 6 below.
41. Ibid.
42. *Paton v Poole Borough Council* (IPT/09/01/C, 29 July 2010), paras 14 and 21.
43. Ibid, paras 43-44.
44. 'The Oversight Role of the Chief Surveillance Commissioner', speech to the Commonwealth Club, 10 February 2009, p5.
45. Ibid, paras 60-73.
46. Ibid, para 65.
47. See Chapter 5 below.
48. Ibid.
49. Hansard, HC Debates cols 634-41, 17 November 1966. Wilson's statement was, however, subject to the following proviso: 'But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement to the House about it'.
50. Hansard, col 96WS, 30 March 2006.
51. Hansard, 173WS, 15 December 2005.
52. *Report of the Interception of Communications Commissioner for 2005-2006* (HC 315, February 2007), paras 47-57.
53. See eg, 'Probe into police 'bugging' of MP', BBC News, 3 February 2008; Sir Christopher Rose, *Report on Two Visits by Sadiq Khan MP to Babar Ahmad at HM Prison Woodhill* (HC 7336, February 2008).

the Wilson Doctrine. However, a report by the Chief Surveillance Commissioner concluded that the surveillance was 'carried out lawfully' under RIPA and that it was 'authorised and fully documented'.[54] The Chief Commissioner further noted that the surveillance did not appear to be covered by the terms of the Wilson Doctrine 'because it does not give rise to interception as defined by the legislation nor would it require authorisation by the Secretary of State'.[55] In her statement to Parliament following the Chief Commissioner's report, the Home Secretary told MPs that the relevant statutory codes of practice under RIPA would be clarified to ensure that discussions with their constituents should be considered as 'confidential information', and treated 'in the same way as conversations between a person and their lawyer or minister of religion'.[56] Despite a Divisional Court ruling in December 2007 that monitoring conversations between lawyers and clients breached Article 8 ECHR,[57] the government failed to change the law until February 2010.[58]

- The number of authorisations for the use of surveillance by the intelligence services over the last decade – whether for property interference, directed surveillance or intrusive surveillance – has never been made public.[59]

- In June 2010, it was revealed that nearly 200 ANPR cameras had been installed in two predominantly Muslim suburbs of Birmingham by West Midlands Police – up to three times as many ANPR cameras as had been installed in the city centre.[60] Following an investigation by a national newspaper, it emerged that the cameras had been installed as part of the force's counter-terrorism unit, with the consent of MI5 and the Home Office. Local community groups had originally been told the cameras were for the purpose of general crime prevention and it was only as a result of the ensuing public outcry that the cameras were removed.[61]

- Between 2000 and 2010, there have been 39,815 covert human intelligence sources recruited, including 1,814 by non-law enforcement bodies such as government departments and local authorities.[62]

- In July 2011, the Court of Appeal quashed the convictions of 20 climate change activists for conspiracy to commit aggravated trespass of Ratcliffe-on-Soar power station following revelations that their protest group was one of a number that had been infiltrated by an undercover police officer named Mark Kennedy and that the Crown Prosecution Service had failed to disclose this at their trial.[63] Among other things, the Lord Chief Justice found that Kennedy 'was involved in activities which went much further than the authorisation he was given, and appeared to show him as an enthusiastic supporter of the proposed occupation of the power station and, arguably, an agent provocateur'.[64] The appeal followed a series of reports in the *Guardian* newspaper in January 2011 which identified Kennedy as one

54. Ibid, para 27.
55. Ibid, para 3.
56. Hansard, HC Debates, 21 February 2008, col 538.
57. *In re McE (Northern Ireland) and others* [2009] UKHL 15.
58. See Chapters 3 and 5 below.
59. See Chapters 4-8 below.
60. 'Surveillance cameras in Birmingham track Muslims' every move' by Paul Lewis, The Guardian, 4 June 2010.
61. 'CCTV aimed at Muslim areas in Birmingham to be dismantled', The Guardian, 25 October 2010.
62. See Chapter 7 below.
63. *David Robert Barkshire and others v The Queen* (Court of Appeal Criminal Division, unreported, 20 July 2011).
64. Ibid, para 18.

of a number of undercover officers with the National Public Order Intelligence Unit who had spent several years infiltrating environmental protest groups.[65] Kennedy's undercover activities alone are estimated to have cost the taxpayer more than £2.25 million.[66]

- Between 2001 and 2010, there have been more than 1,000 complaints (1,120) concerning unwarranted or excessive surveillance by public bodies including the police and the intelligence services to the IPT.[67]

- Out of more than 1,000 complaints over the last decade, only 10 have been upheld by the Tribunal.[68]

11. Concern over the extent of surveillance powers now extends far beyond the traditional constituency of civil liberties groups and privacy campaigners. In 2006, the first Information Commissioner said that the UK was 'sleepwalking into a surveillance society'.[69] In 2008, the former Director of Public Prosecutions warned that the government's proposed Communications Data Bill would be 'an unimaginable hell-house of personal private information'.[70] In the same year, the House of Commons Home Affairs Committee issued its report warning of the dangers of the UK becoming a surveillance society.[71] The same warning was repeated by the House of Lords Constitution Committee in its report the following year.[72] Concerns over excessive surveillance dominated the Convention on Modern Liberty held in February 2009, and featured heavily in the election manifestos of the Conservative and Liberal Democrats in the 2010 General Election.[73] The Coalition Programme for Government, published following the election, promised among other things to 'implement a full programme of measures to reverse the substantial erosion of civil liberties and roll back state intrusion', including to 'scrap the ID Card scheme', 'end the storage of Internet and email records without good reason', and 'further regulate CCTV'.[74] In January 2011, the Home Office published its review of counter-terrorism powers which included recommendations to 'end the use of the most intrusive RIPA powers by local authorities to investigate low level offences', a requirement that 'applications by local authorities to use any RIPA techniques are approved by a magistrate', as well as 'commitment to rationalise the legal bases by which communications data can be acquired and, as far as possible, to limit that to RIPA'.[75] In February 2011, the government introduced its Protection of Freedoms Bill in Parliament, containing several proposed amendments to RIPA.

---

65. See eg, 'Undercover officer spied on green activists', the *Guardian,* 9 January 2011; 'Spying on protest groups has gone badly wrong, police chiefs say', the *Guardian,* 19 January 2011.
66. See eg, the *Daily Mail,* Farce of the £2m eco-activist undercover police operation , 18 April 2011.
67. See Chapter 9 below.
68. Ibid.
69. BBC News, 'Watchdog's Big Brother UK warning', 16 August 2004.
70. See eg, 'Private firm may track all email and calls', the *Guardian,* 31 December 2008.
71. House of Commons Home Affairs Committee, *A Surveillance Society?* (HC 58, 8 June 2008).
72. House of Lords Constitution Committee, *Surveillance: Citizens and the State* (HL 18, 6 February 2009).
73. See eg, the Conservative Party Manifesto 2010 which referred to the Labour government having 'trampled on liberties and, in their place, compiled huge databases to track the activities of millions of perfectly innocent people, giving public bodies extraordinary powers to intervene in the way we live our lives'. It included a specific promise to curtail 'the surveillance powers that allow some councils to use anti-terrorism laws to spy on people making trivial mistakes or minor breaches of the rules' (p79). Similarly, the Liberal Democrat's 2010 Manifesto asserted that '[d]ecades of Labour and Conservative rule have overthrown some of the basic principles of British justice and turned Britain into a surveillance state' and promised to 'regulate CCTV, stop councils from spying on people ... and stop children being fingerprinted at school without their parents' permission' (p93).
74. *The Coalition: Our Programme for Government* (May 2010), p11.
75. Home Office, *Review of Counter-Terrorism and Security Powers: Review Findings and Recommendations* (Cm 8004, January 2011), p5.

12. This report argues, however, that piecemeal amendment of RIPA is not enough. Even if all the amendments proposed by the Protection of Freedoms Bill are enacted, RIPA will continue to provide a wholly inadequate legal framework for surveillance. What is needed instead is root-and-branch reform: a Regulation of Surveillance Act that is clear, coherent and no more complex than it needs to be; an Act that ensures that decisions about surveillance are made by independent judges rather than politicians; an Act that provides effective oversight rather than the seemingly endless proliferation of part-time commissioners; an Act that promotes accountability and public trust rather than corrodes it; and an Act that is principled, proportionate and effective.

13. This report builds on our 1970 and 1998 reports by examining in detail the provisions and operation of RIPA, analysing the key issues and presenting recommendations for reform:

- Chapter 2 introduces some key concepts (eg, privacy and surveillance), and outlines the relevant legal standards under UK and European law, in particular the right to respect for private life under Article 8 ECHR;

- Chapter 3 looks at the interception of communications – the covert acquisition of the contents of a phone call, email, letter, etc. while it is being delivered – under Part 1 of RIPA, including the criminal offence of interception, the issue of interception warrants by government ministers, and the current ban on the use of intercepted material as evidence;

- Chapter 4 deals with the power of a wide range of public bodies to obtain communications data – so-called 'envelope' data concerning the sending and receipt of phone calls and emails, the increasingly blurred line between envelope data and actual content, and the amendments proposed by the Protection of Freedoms Bill;

- Chapter 5 examines 'intrusive' surveillance under Part 2 of RIPA – surveillance which involves intrusion into a person's home, vehicle or office, and the role of the Surveillance Commissioners in the authorisation process;

- Chapter 6 deals with 'directed' surveillance under Part 2 – surveillance by public bodies which does not involve intrusion into property, etc. – along with the reforms proposed by the Protection of Freedoms Bill;

- Chapter 7 concerns the authorisation and use of covert human intelligence sources (or 'CHISs'), including the use of informants and undercover police officers;

- Chapter 8 looks at the power of the police to demand encryption keys – used to prevent computer data from being read by anyone other than its owner – under Part 1 of RIPA, including the long delay in introducing the power and the relationship with the debate on pre-charge detention in terrorism cases;

- Chapter 9 looks at the role of the various oversight commissioners under RIPA as well as the IPT, including the judgment of the ECHR in *Kennedy v United Kingdom*;

- Chapter 10 summarises the arguments in favour of wholesale reform of RIPA and presents recommendations to serve as the basis for a draft Surveillance Reform Bill.

KEY TERMS

14. This report is written for a general audience. Unfortunately, though, the law governing surveillance is not. This section, therefore, sets out some of the key terms, particularly for the benefit of non-lawyers.

Interception of communications

15. 'Interception of communications' is the technical term for covert acquisition of the *contents* of messages or conversation that has been carried over a communications network or delivered by a service. The best known examples of this are phone tapping (eg, traditionally done via wiretaps but now carried out digitally) or phone hacking (secretly accessing another person's voicemail).[76] 'Interception', however, covers any kind of communications network, public or private, and includes email, faxes, text messages and ordinary post.

16. It is important to be clear that *interception* only applies to communications travelling across some kind of network or via a service. If, for example, someone opened and read a letter addressed to Mr White while it was being processed through Royal Mail's sorting office, that would count as an interception of Mr White's mail. If, however, someone broke into Mr White's house and read the same letter while it lay open on his desk, that would certainly involve a serious invasion of Mr White's privacy (not to mention his house) but it would not qualify as an interception. Similarly, if the police were to direct Mr White's phone company to record his telephone calls, that would involve an interception. If, though, the police planted a secret listening device (or bug) in Mr White's house and – as a result – recorded those same phone conversations, that would certainly amount to 'intrusive' surveillance under RIPA, but it would not be an interception.

17. As will be looked at in Chapter 3 below, uncertainty about the definition of 'interception' under RIPA appears to have been a major factor in the failure of the Metropolitan Police to properly investigate allegations of widespread phone hacking by the *News of the World.*

Communications data

18. Communications data – sometimes known as 'envelope data' – is *information about* a message that has been sent via a network or service, as opposed to the *contents* of that message.

19. For an ordinary piece of post, for example, communications data is literally the information that can be obtained from the envelope, ie, the address it was sent to, the postmark showing where it was received and sorted, and – where available – the sender's address. In the case of phonecalls or email, however, so-called 'envelope data' is a great deal more substantial because of the wealth of information that is nowadays regularly logged by ISPs and phone companies, including, in the case of mobile phones, the name, address and account details of the caller and the person called, the make of their mobile phones, and any geolocation data.

---

76. The practice of interception is, however, extremely old: the first public reference to the Secretary of State authorising the opening of letters via warrant was in 1663; President Lincoln apparently authorised the tapping of telegraphs during the American Civil War and in *Malone v United Kingdom* (1984) 7 EHRR 14, the European Court of Human Rights noted that 'the power to intercept telephone messages has been exercised in England and Wales from time to time since the introduction of the telephone' (para 28).

20. Generally speaking, the law treats the interception of communications as a much more serious interference with privacy than access to communications data. However, in many cases, the information *about* a phone call, eg, the time the call was made, who it was made to, how long the call lasted and so forth, can be far more useful to investigators than what was actually said.

'Directed' and 'intrusive' surveillance

21. RIPA defines surveillance as 'covert' if 'and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place'.[77] It goes on to distinguish between two kinds of covert surveillance that may be carried out by public authorities: 'directed' and 'intrusive' surveillance.

22. 'Directed' surveillance is covert surveillance 'likely to result in the obtaining of private information about a person' but which does not involve an intrusion into anyone's home or privately-owned vehicle.[78] So, for example, following a person down a street and making notes about his activities, or deliberately overhearing someone else's conversation on a park bench, would be garden-variety instances of 'directed' surveillance under RIPA. It may also include, however, tracking a vehicle's location[79] and external video surveillance of a person's vehicle or home.[80]

23. 'Intrusive' surveillance is, by contrast, surveillance carried out by a covert device placed in a person's home or vehicle,[81] typically 'sound or video eavesdropping in someone's house or car'.[82] Since 2009, the government has accepted that surveillance of a consultation between a lawyer and client, wherever it takes place, also qualifies as 'intrusive' surveillance.[83]

'Covert human intelligence source'

24. 'Covert human intelligence source' ('CHIS') is the term used by RIPA for any person who acts as an informant or an undercover agent on behalf of a public body – whether police, intelligence services or even a local authority.[84] At one extreme, this would include, for instance, an MI5 officer posing as a would-be terrorist in order to infiltrate a suspected Al Qaeda cell. At the other extreme, this definition would also include, for example, a postal worker who, unbeknownst to his colleagues, had secretly agreed to pass on information concerning their activities to his superiors, as part of a workplace investigation into potential criminal activity.

25. The essential feature of any so-called CHIS for the purposes of RIPA is the maintenance of a 'relationship' – whether personal, professional or otherwise – where it is conducted in a manner

---

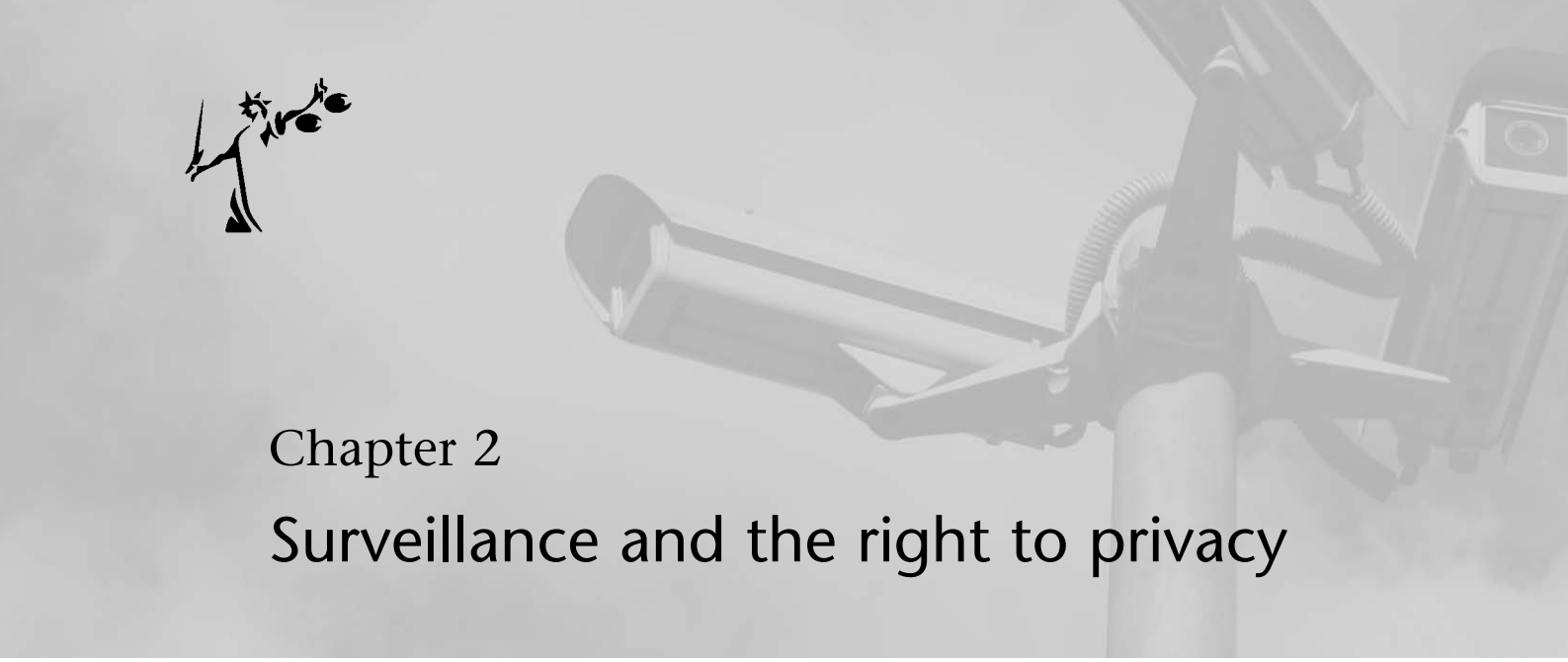
77. Section 26(9) of RIPA.
78. Section 26(2) of RIPA.
79. Section 26(4)(a) of RIPA.
80. Unless the surveillance device 'is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle' (section 26(5) of RIPA).
81. Or, exceptionally, an external surveillance device capable of obtaining information 'of the same quality and detail' as an internal device: see ibid.
82. *Report of the Intelligence Services Commissioner for 2002* (HC 1048, para 24, September 2003).
83. See *In re McE* [2009] UKHL 15, per Lord Hope at para 60: 'The Secretary of State now accepts that directed surveillance of legal consultations in detention should be treated as intrusive surveillance for the purposes of prior authorisation under Part II of RIPA'.
84. See section 26(8). See also eg, *Report of the Intelligence Services Commissioner for 2001* (HC 1244, October 2002), para 26: 'Covert human intelligence sources are essentially people who are members of or act on behalf of one of the intelligence services to obtain information from people who do not know that this information will reach the intelligence service'.

'calculated to ensure' that the other person or persons are unaware of its true purpose.[85] In other words, it includes any situation where one person in a relationship has agreed to secretly pass on information about the other person to a public authority, eg, a husband informing on his wife, a worker informing on his colleagues, a student on his teachers, etc.

Encryption keys

26. Broadly speaking, an encryption key is any piece of information that enables encrypted material to be decoded (eg, a key to a crossword). The sophistication of modern encryption software poses a particular challenge for investigators, however, so Part 3 of RIPA provides for the power of authorities to require a person in possession of electronically encrypted material to provide the relevant 'key, code, password, algorithm or other data' that enables the material to be accessed or put into intelligible form.[86] This may nowadays include not only computer passwords, etc., but even voice-activation codes or the biometric data from a fingerprint scan.[87]

85. Section 26(9)(b).
86. Section 56(1) of RIPA. The power to require an encryption key extends to 'any person' that the authorities believe has the appropriate key (section 49(2)).
87. Home Office, *Investigation of Protected Electronic Information: Code of Practice* (2007), para 3.19. See further Chapter 8 below.



Chapter 2
Surveillance and the right to privacy

Privacy as a public good

27. In the debate over surveillance, it is often assumed that the balancing of interests involves a straightforward clash between the relevant public interest (eg, national security or the prevention and detection of crime) on the one hand, and the individual's interest in preserving his or her privacy on the other.

28. This is a mistake, however; one that relies on a false opposition between the public interest and the right to privacy. The better view is that privacy as a right protects not only the interest of each person in their own privacy but also its general importance as a *public* good. By this we mean that there is a collective interest in maintaining a society in which personal privacy is protected. There are a number of reasons for this, not the least of which is that a free society is one that respects individual freedom to live a life without undue interference or scrutiny. Another, closely associated with this, is that our very ability to make autonomous decisions depends to a significant extent on having sufficient social space in which to deliberate about them. A third reason is the belief that individuals are more likely to contribute to the maintenance of a good society where they recognise that that society is concerned with protecting their own rights, including the right to privacy.

29. Just as we value freedom of speech for giving rise to the free and open exchange of ideas and information in the public domain, therefore, so too do we value privacy as a zone (or, more accurately, a series of overlapping zones) in which people are not required to share information with the world at large.

30. The maintenance of privacy as a collective good, however, requires not only governmental action but also restraint. On the one hand, the government has an obligation to protect people's privacy from unnecessary intrusion by others, eg, phone hacking. On the other hand, the power of the authorities to investigate criminality – including, eg, by secretly intercepting the phone calls of suspected phone hackers[88] – also needs to be subject to the strictest controls, lest it undermine the very public good it is meant to preserve.

---

88. See eg, 'Phone hacking: Rebekah Brooks faces questioning', by Vikram Dodd, the *Guardian,* 11 April 2011: during an earlier inquiry Scotland Yard was so concerned by allegations that the paper was paying bribes to serving officers and other key workers that it tapped Brooks's telephone. Police found no evidence that she had committed any offence. The tapping of her phone was carried out with a Home Office warrant early in 2004 as part of an inquiry by Scotland Yard's anti-corruption command into allegations that the News of the World was bribing serving officers, buying confidential data from the police national computer and making regular cash payments of up to £1,000 a week to employees of phone companies who were selling information from the accounts of public figures .

What is surveillance?

31. Covert observation is probably one of the oldest kinds of human activity. The idea of privacy, by contrast, likely dates only from the time when human beings first lived under conditions that allowed for some measure of privacy. Certainly, the two concepts have a long history. For, in order for something to be considered private, there must also exist the possibility of that privacy being intruded upon.

32. For its part, the Oxford English Dictionary defines surveillance as 'close observation, especially of a suspected spy or a criminal'. Surveillance, then, is something typically used against people who are engaged in underhand or illegal activities. But – perhaps because surveillance itself is at its most effective when it is carried out covertly and because it can involve serious breaches of privacy – the very act of surveillance also has the connotation of being underhand. Even lawful surveillance, therefore, involves an element of fighting fire with fire – the idea that it may be legitimate to adopt covert methods and invade the privacy of others for the sake of some greater good, such as apprehending a dangerous terrorist.[89]

33. If surveillance is a very old activity, however, our concept of surveillance has nonetheless broadened considerably over the last century. In 1911, for example, surveillance was something incapable of being carried out either remotely or automatically. It was primarily a physical activity undertaken by individuals (eg, a police officer) that would be focused either on a specific person (eg, John Smith) or place (eg, 221 Baker Street). In an exceptional case, surveillance might also involve the interception of post and telephone calls but neither activity was capable of being automated. Perhaps the most sophisticated surveillance device in 1911 was the dictograph – the adaptation of a telephone receiver to work as a hidden microphone – but it was a very early technology. At the same time, the government of the day might also have in its possession various pieces of information about both John Smith and/or 221 Baker Street. But the nature of record-keeping and government administration meant that it would have been possible to gather all available information held by various public bodies about John Smith or 221 Baker Street only with extraordinary difficulty.

34. The last century has seen three key developments in surveillance. First, technological advances have made surveillance far more effective, both in terms of the ability to gather information about a subject as well as for that activity to be carried out without detection. In place of dictographs and postal intercepts, for instance, there is now the possibility of covert sound and video recording; digital interception of mobile phones, texts, emails, etc.; biometric measures, such as DNA sampling and facial recognition software; and aerial and even satellite surveillance. Second, as technology has advanced, it has become correspondingly easier for both public and private bodies to gather, store and transfer greater and greater amounts of data about individuals. Third, the sheer size of government – as well as its powers, functions and capabilities – has grown enormously. In 1911, for instance, the newly-founded Secret Service Bureau had a staff of ten but was characterised as being 'an agency of one man'.[90] In 2011, by contrast, the Bureau's successor agencies – MI5, MI6

89. Not all surveillance need be covert, of course. Simply standing on a street corner and recording information about everyone who walks past may count as surveillance, in a sense.
90. Philip Davies, *MI6 and the Machinery of Spying* (Cass, 2004) at p39: 'Despite briefings from Edmonds, eventual on-site access to MO5's operational files and even inheriting a small stable of agents, [Captain Mansfield Smith-Cumming] found himself, otherwise, an agency of one man'. In fact, by 1911 the Bureau had already unofficially divided itself in two: foreign intelligence under the direction of Smith-Cumming and domestic intelligence under the direction of Captain Vernon Kell. This internal division was later made official by the establishment of MI5 and MI6 as separate entities. The origins of GCHQ were separate, evolving from the work of the Government Code and Cypher School, founded in 1919.

and GCHQ – employ more than 12,000 people between them,[91] with a combined budget of more than £2 billion.[92]

35. Together, these developments mean that surveillance is no longer necessarily a sustained human activity but something that is capable of being carried out on an automated and indeed systemic basis. A good example of this is Britain's network of Automated Number Plate Recognition (ANPR) cameras whose coverage extends to most motorways and town centres in the UK. Every time a car, motorbike, van or truck comes within range of an ANPR camera, its licence plate, together with the time, date and location of the vehicle, is automatically logged and checked against a number of local and national police databases, including the Police National Computer, the DVLA and the Motor Insurers' Bureau. According to the National Policing Improvement agency, this 'ensures officers are alerted, in real time, to vehicles that are stolen, involved in crime, unregistered, unlicensed or uninsured'.[93] With more than 100 million 'reads' each week, the ANPR network involves surveillance on a massive scale but is also almost entirely an automated activity in which any individual driver will not normally be the subject of active surveillance by a human operator unless the system flags a vehicle as stolen or uninsured, etc.

36. There is a great deal more to the ANPR network than just flagging stolen vehicles, however, as it can also be used by the police and other agencies to carry out real-time surveillance of particular suspects. More generally, the massive amounts of data gathered by the ANPR network each day makes it an incredibly powerful investigative tool. For every vehicle sighting is not only crosschecked but also stored by the Police National ANPR Data Centre in Hendon, meaning that it becomes possible for the police to track not only a single journey of a particular vehicle on a given day (eg, the route taken by John Smith's car between London and Birmingham on 2 October) but also, over time, how that vehicle is used generally (eg, every trip John Smith's car made in the last 12 months, their length and frequency, etc). As the Chief Constable of Hertfordshire Police, Frank Whiteley, told one newspaper in 2005:[94]

> We can use ANPR on investigations or we can use it looking forward in a proactive, intelligence way. Things like building up the lifestyle of criminals - where they are going to be at certain times. We seek to link the criminal to the vehicle through intelligence. Vehicles moving on the roads are open to police scrutiny at any time.

Indeed the ANPR network shows how, in some cases, automated surveillance may, over time, gather a great deal more information about an individual's activities than short periods of active surveillance. Why follow someone for 24 hours, for instance, when a request to the ANPR Data Centre will reveal his car journeys over the past year?

37. It isn't necessary, however, for a system to be *designed* for surveillance purposes – as ANPR is – in order to be *useful* for surveillance. For example, although Transport for London operates more than 20,000 CCTV cameras in its buses and Underground stations,[95] its Oyster card system is equally

---

91. MI5 employs approximately 3,800 people, MI6 about 2,000 and GCHQ about 5,500: see eg, www.mi5.gov.uk/output/staff-and-management.html.
92. HM Treasury, *Spending Review 2010* (Cm 7942, October 2010), p75.
93. See www.npia.police.uk/en/10505.htm.
94. 'Surveillance UK: why this revolution is only the start' by Steve Conner, the *Independent*, 22 December 2005.
95. See response of Transport for London to a request under the Freedom of Information Act, dated 16 November 2009: TfL operates approximately 13,000 cameras on the Underground, over 8,000 on buses operated by the various bus companies contracted to it, and a further 1,336 on the Overground, Docklands Light Railway and Trams.

capable of providing similar data on the movements of any particular cardholder, eg, how many times a week does John Smith enter or exit Westminster Tube station? It does not matter that the information is not gathered for the purposes of surveilling people. The fact remains that the data accumulated about each individual user has tremendous forensic value to anyone with access to it. And the same is true for the personal data gathered and retained by most every public body – and many private companies – in the UK. As we predicted in our 1970 report, the rise of computer networks meant that it was 'only a matter of time before … all information on any individual stored anywhere within the network can be made available in one print-out at the press of the appropriate button'.[96] And in a society in which every electronic transaction, search entry, webpage visit, tube ride, car journey and email is logged and stored somewhere, 'all information on any individual' can be considerable indeed.

38. 'Surveillance', therefore, now not only means the 'active' surveillance of a person - in the sense of a person being actively watched by other persons – but also the 'passive', automated surveillance of a person that occurs simply by virtue of living in a society in which large amounts of data about individuals is routinely gathered and stored by a wide range of public and private bodies on a daily basis.[97] And it is the ubiquity of 'passive' forms of surveillance which has given rise in recent years to various descriptions of the UK as a 'surveillance society' or 'surveillance state'.[98]

39. This broadening of the concept of surveillance poses a particular challenge for the law, for RIPA is almost entirely concerned with 'active' surveillance, ie, the focused investigation of particular suspects by a range of public bodies rather than the general business of large-scale data gathering. The latter is instead regulated by the various Data Protection Acts and associated EU measures such as the E-Privacy Directive. This division of legislative labour may seem reasonable enough, for data has many other uses besides surveillance. But it is also plainly problematic that so much of what nowadays falls under the broader definition of surveillance should nonetheless fall outside the scope of the very statute meant to regulate it.

40. In order to better understand the framework established by RIPA, however, it is important to first consider: i) how privacy was traditionally protected by the common law; and ii) the difference that has been made by the HRA 1998 and, in particular, the protections of Article 8 ECHR.

Privacy and the common law

41. In a 2010 decision of the Northern Irish High Court concerning RIPA, Lord Justice Girvan opened his judgment with a quote from *Richard III*, in which Richard declares 'Under our tents I'll play the eavesdropper, To hear if any mean to shrink from me'. Girvan goes on to explain:[99]

96. See n3 above.
97. See eg, House of Lords Constitution Committee, *Surveillance: Citizens and the State*, n72 above, paras 24-25.
98. In an interview with the *Times* in August 2004, the first Information Commissioner Richard Thomas warned that the UK risked 'sleepwalking into a surveillance society' due to government plans for identity cards, the Citizen's Information Project proposed by ONS, and the childrens database: 'My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than British society would feel comfortable with'. ('Beware rise of Big Brother state, warns data watchdog', by Richard Ford, the *Times*, 16 August 2004). Two years later, following the enactment of the Identity Cards Act 2006, the Commissioner gave another interview in which he said that his fears had become a reality. (BBC News, 'Britain is 'surveillance society', 2 November 2006).
99. *Re A's Application* [2010] NIQB 99 at para 1.

> *It is unsurprising that amongst the malign characteristics Shakespeare attributes to Richard III in his entirely negative portrayal were those of an eavesdropper. In Shakespeare's time and to this day eavesdropping was and is regarded as an essentially objectionable invasion of the privacy which citizens are entitled to expect and a trespass upon the personal space of individuals who are entitled to be free from prying ears and eyes.*

In fact, in both Shakespeare's time and – until very recently[100] – our own, eavesdropping was an offence at common law. As Blackstone explained:[101]

> Eaves-droppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet: or are indictable at the sessions, and punishable by fine and finding sureties for the good behaviour.

Girvan makes no reference to this. Nor, despite its criminality, does he concede that eavesdropping was a very popular plot device in Shakespeare's plays, and not restricted to villains. But his essential point remains sound. Like such folk figures as Peeping Tom (from the legend of Lady Godiva) and the Nosy Parker (apocryphally named for Matthew Parker, Elizabeth I's Archbishop of Canterbury, known for his zealous use of search warrants in order to recover religious works from the private libraries of collectors),[102] the eavesdropper epitomises a type of intrusion that has been objectionable for at least as long as there has been an English language. And the ancient offence of eavesdropping reflects the equally long-standing concern of English law to protect personal privacy.

42. However, the common law's protection of privacy has never been direct, at least in the sense of privacy itself being a justiciable right. Instead, it has historically been protected by one of two means: i) the occupation of property; and ii) the law governing confidential information. In the first case, the common law provided a range of protections against intrusion, whether by way of the criminal law or such torts as trespass and nuisance. Hence Sir Edward Coke's famous statement that 'a man's house is his castle',[103] and Pitt the Elder's subsequent elaboration of it in 1763:[104]

> The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter, the rain may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement.

---

100. The offence of eavesdropping was abolished by section 13(1) of the Criminal Law Act 1967. The Law Commission had earlier recommended its abolition on the grounds that 'neither the pocket listening device, the modern menace of 'bugging' nor the 'peeping Tom' type of offence can be made to fit into this ancient misdemeanour so as to justify its retention. Nuisances of the 'peeping Tom' kind have in fact been dealt with satisfactorily by magistrates by the exercise of their powers to bind over'. (Law Commission of England and Wales, *Proposal to Abolish Certain Ancient Criminal Offences* [1966] EWLC 3, at para 3). There are now a variety of specific offences dealing with similar types of conduct: see eg, voyeurism contrary to section 67 of the Sexual Offences Act 2003.
101. *Commentaries on the Law of England,* Bk IV, Ch 13. See also eg, *Tomlins' Law Dictionary*, 4th ed (1835) which refers to the 'particular and tender regard which the law of England has to a man's house', which is taken to explain 'in part the animadversion of the law upon eaves-droppers, nuisancers, and incendiaries'.
102. According to Corpus Christi, Parker's college at Cambridge, he obtained a warrant from the Privy Council to 'make a general search after all such records and muniments as related to these Realms, and which upon the dissolution of the monasteries had fallen into private hands; whereby he preserved from perishing some of the most valuable remains of our Church and Nation' and in doing so incurred the general hostility of the owners of many private book collections. See www.corpus.cam.ac.uk.
103. *Institutes of the Laws of England,* III (1628), p162: 'for a man's house is his castle, *et domus sua cuique est tutssimum refugium*; for where shall a man be safe, if it be not in his house?'. See also *Semayne's Case,* 77 Eng. Rep. 194, 195; 5 Co. Rep. 91, 195 (KB, 1604): 'the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose'.
104. Speech on the Excise Bill, House of Commons, March 1763.

Similarly, Lord Camden's speech in the 1705 judgment in *Entick v Carrington* upheld the rights of property owners against unlawful searches by the executive:[105]

> By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing; which is proved by every declaration in trespass, where the defendant is called upon to answer for bruising the grass and even treading upon the soil.

This line of common law principle became the basis for the guarantees of the Fourth Amendment to the US Constitution, providing that the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated'. American courts subsequently identified an actionable right to privacy under both common law[106] and the US Constitution.[107]

43. The second traditional ground for the protection of privacy under the common law has been the law governing confidentiality, used to prevent the unauthorised use of confidential information.[108] So, for instance, an action for breach of confidence would enable the granting of an injunction to prevent the publication of a person's medical records. As Lord Eldon said in 1820 concerning an engraving of George III during one of his periods of madness, 'if one of the late king's physicians had kept a diary of what he heard and saw, the court would not, in the king's lifetime, have permitted him to print and publish it'.[109] In some cases, the protection the common law gave to confidential information was reinforced by statute: the Post Office Act 1710, for instance, forbade the opening of letters save under warrant. However, the power of ministers to direct the opening of mail was apparently much abused, as Lord Lyttelton complained in 1735:[110]

> If we have so much Reason to be unwilling, that what we *Print* shou'd be under *Inspection* of the Court; how much more may we complain of a new Power assumed within these last fifty Years by all the Courts of *Europe*, of *inspecting private Letters*, and invading the *Liberty of the Post?* The Secrecy and Safety of Correspondence, is a Point of such Consequence to Mankind, that the least Interruption of it wou'd be

105. 19 Howell's State Trials 1029, 95 Eng. 807 (1705).
106. See eg, the seminal article by Warren and Brandeis, 'The Right to Privacy' (1890) 4 Harvard LR 193. US law today recognises no less than four kinds of invasion of privacy: (1) intrusion on physical solitude; (2) public disclosure of private facts; (3) publicity putting the plaintiff in a false light; and (4) appropriation of another's name and likeness: see Prosser, *Law of Torts,* 4th ed (1971) p804. See also our 1970 report, n2 above, paras 119-121: 'It is a fact little-known in England that the whole of the extensive law of privacy which has been developed in the USA has its roots, indirectly, in the common law of England .... [However] in the absence of a large class of rich private plaintiffs who feel strongly enough about their privacy – or a large class of very poor such plaintiffs, combined with abundant legal aid and enough bold lawyers – it seems likely that very many years would be required to bring the law of privacy in England to the point which it has reached in the USA today. And that, in our view, would be far too late'.
107. See eg, the decisions of the US Supreme Court in *Griswold v Connecticut* 381 US 479 (1965), Rowe *v Wade* 410 US 113 (1973), and *Lawrence v Texas* 539 US 558 (2003).
108. See eg, the submissions of the Solicitor General in *Prince Albert v Strange* [1849] EWHC Ch J20 (8 February 1849): 'That there is property in the ideas which pass in a man's mind is consistent with all the authorities in English law. Incidental to that right is the right of deciding when and how they shall first be made known to the public. Privacy is a part, and an essential part, of this species of property'. Lord Cottenham LC accepted that where 'privacy is the right invaded, the postponing of the injunction would be equivalent to denying it altogether'.
109. *Wyatt v Wilson* (1820), unreported, cited in *Prince Albert v Strange,* ibid.
110. *Letters from a Persian in England, to his Friend at Ispahan* (1735), Letter 51. See also Erskine May, n1 above, p292: 'Akin to the use of spies, to watch and betray the acts of men, is the intrusion of government into the confidence of private letters, entrusted to the Post-office. The state having assumed a monopoly in the transmission of letters on behalf of the people, its agents could not pry into their secrets without a flagrant breach of trust, which scarcely any necessity could justify. For the detection of crimes dangerous to state or society, a power of opening letters was, indeed, reserved to the secretary of state. But for many years, ministers or their subordinate officers appear to have had no scruples in obtaining information, through the Post-office, not only of plots and conspiracies, but of the opinions and projects of their political opponents. Curiousity more often prompted this vexatious intrusion than motives of public policy'.

> criminal, without an evident *Necessity*; but that of Course, from one Year to another, there shou'd be a constant Breach of it publickly avow'd, is such a Violation of the Rights of Society, as one cannot but wonder at *even at this Age* …. I beg you to inform me what it was, that cou'd induce a free People to give up all the Secrets of their Business and private Thoughts, to the Curiosity and Discretion of a Minister, or his inferior Tools in Office?

By the 1970s, this practice had become the basis not only for interception by the authorities of post but telephone calls as well. Yet, as Sir Robert Megarry held in the 1979 case of *Malone v Commissioner of Police for the Metropolis*, there was nothing in the doctrine of confidentiality or the common law in general that provided a particular right of privacy in respect of phone conversations.[111]

44. The law governing confidentiality provided only partial protection for privacy in other respects too. In particular, an action for breach of confidence traditionally depended on there being some pre-existing relationship of confidentiality between the parties, eg, doctor-patient, lawyer-client, etc. However, in a 2004 case involving the *Daily Mirror's* publication of photos of Naomi Campbell leaving a meeting of Narcotics Anonymous, the House of Lords unanimously confirmed that the cause of action was no longer restricted to cases involving a confidential *relationship*.[112] A majority of the House also concluded that her attendance at NA meetings constituted 'private information which imported a duty of confidence'.[113] Moreover, the traditional label of 'breach of confidence' was itself no longer accurate, as Lord Nicholls explained:[114]

> The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. *The essence of the tort is better encapsulated now as misuse of private information. In the case of individuals this tort, however labelled, affords respect for one aspect of an individual's privacy. That is the value underlying this cause of action.*

45. In the years since *Campbell* was decided, there has been a veritable explosion in the number of interim injunctions granted on behalf of celebrities and public figures seeking to prevent breaches of their private information.[115] And, as we will see below, this development of the traditional equitable doctrine of breach of confidence into a modern tort of misusing of private information is almost entirely due to the impact of Article 8 ECHR following the enactment of the HRA.[116] But the Law Lords have so far continued to resist recognising a general tort of invasion of privacy, unanimously rejecting such a development in the 2003 appeal of *Wainwright and another v Home Office*.[117]

---

111. *Malone v Commissioner of Police for the Metropolis* [1979] 244 Ch 357-362. See below for further discussion of *Malone v United Kingdom* (1984) 7 EHRR 14. See also eg, the statement of Lord Nolan in *R v Khan* (1996) 3 WLR 162 at 175 concerning the admissibility of evidence obtained via unlawful surveillance: 'under English law, there is in general nothing unlawful about a breach of privacy'.
112. *Campbell v MGN Limited* [2004] UKHL 22. See also eg, *Attorney-General v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 at 281 per Lord Goff.
113. *Campbell,* ibid, para 95 per Lord Hope.
114. Ibid, paras 14-15. Emphasis added. See also eg, *OBG Ltd v Allan and others* [2007] UKHL 21 at para 272 per Lord Walker: 'the law of confidentiality has been, and is being developed in such a way as to protect private information'.
115. See eg, *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446.
116. See eg, Report of the Committee on Super-Injunctions, *Super-Injunctions, Anonymised Injunctions and Open Justice* (May 2011), para 12: 'Disquiet about the increasing use of injunctions, and the development of super-injunctions and anonymised injunctions, to protect private information, is, similarly, significantly attributable to the increased ability to protect such information as a consequence of developments in the substantive law following the HRA'.
117. [2003] UKHL 53.

As Lord Hoffmann said in that case:[118]

> There seems to me a great difference between identifying privacy as a value which underlies the existence of a rule of law (and may point the direction in which the law should develop) and privacy as a principle of law in itself. The English common law is familiar with the notion of underlying values - principles only in the broadest sense - which direct its development. A famous example is *Derbyshire County Council v Times Newspapers Ltd* [1993] AC 534, in which freedom of speech was the underlying value which supported the decision to lay down the specific rule that a local authority could not sue for libel. But no one has suggested that freedom of speech is in itself a legal principle which is capable of sufficient definition to enable one to deduce specific rules to be applied in concrete cases. That is not the way the common law works.

46. The protection afforded to privacy by the common law has in any event been increasingly hedged in by statute over the past century. And it is the fact that the common law can be overridden by contrary Act of Parliament that has always been its greatest weakness as a means of protecting fundamental rights. The principle that an Englishman's home is his castle has given way to more than 1,200 statutory powers of entry.[119] As Lord Bingham wrote:[120]

> [I]t is plain that an Englishman's house is now a great deal more porous than Coke and Chatham ever conceived … The common law was powerless to prevent the unregulated interception by the state of private telephone conversations until an adverse decision of the European Court compelled the government to legislate. The common law also developed no coherent rules to protect privacy, while protecting duties of confidence and, for instance, the privacy of a prisoner's correspondence with his legal advisers.

47. And, as we concluded in our 1970 report, such tools that the common law *did* provide to protect privacy have proved increasingly ineffective in dealing with modern forms of surveillance:[121]

> English law does … provide a remedy for some kinds of intrusion into privacy, but it is certainly not adequate to meet the activities of a society which is perfecting more and more sophisticated techniques for intrusion.

Although there have been a number of developments since 1970, the common law has remained a wholly inadequate check against unlawful, unnecessary or disproportionate surveillance. It has instead fallen to the provisions of Article 8 ECHR and, ironically, statute law itself to provide the necessary protection.

---

118. Ibid, para 31. See also eg, Lord Scott at para 62: 'whatever remedies may have been developed for misuse of confidential information, for certain types of trespass, for certain types of nuisance and for various other situations in which claimants may find themselves aggrieved by an invasion of what they conceive to be their privacy, the common law has not developed an overall remedy for the invasion of privacy'; and Lord Hoffmann's speech in *Campbell*, n112 above, para 43: 'the right to privacy is in a general sense one of the values, and sometimes the most important value, which underlies a number of more specific causes of action, both at common law and under various statutes. One of these is the equitable action for breach of confidence, which has long been recognised as capable of being used to protect privacy'.
119. See Explanatory Notes for the Protection of Freedoms Bill as introduced to the House of Commons on 11 February 2011, para 31: 'There are around 1200 separate powers of entry contained in both primary and secondary legislation'.
120. Tom Bingham, *The Rule of Law* (Allen Lane, 2010), pp 75-76. See also eg, *In re McE* [2009] UKHL 15 per Lord Phillips at para 14: 'Prior to 1985 this country failed to comply with Art 8 in as much as the police and the security services intercepted mail and telecommunications and carried out electronic surveillance in accordance with executive discretion that was not subject to statutory regulation'.
121. N2 above, para 85.

Article 8 and UK law

48. Article 8 ECHR provides:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

49. The UK *government* had been bound by its obligations under Article 8 since the Convention came into force in September 1953. This included the duty of the government to abide by the final judgments of the European Court of Human Rights (ECtHR) in any case to which it was party.[122] For several decades, however, the Convention remained unincorporated by Parliament, meaning that the UK *courts* were unable to give effect to the rights it contained. This changed with the HRA 1998, which came into force in October 2000 and enabled UK courts to give effect to Convention rights through a variety of means (although it stopped well short of allowing the courts to strike down inconsistent legislation).[123]

50. Even before the Act came into force, though, Article 8 of the ECHR had already been influencing the development of UK law for a number of years due to the impact of rulings by the ECtHR in Strasbourg. As Lord Bingham noted, it was the 1982 judgment of the Strasbourg Court in *Malone* that prompted the government to introduce the Interception of Communications Act 1985.[124] The Security Service Act 1989 was introduced following an admissibility ruling by the European Commission of Human Rights in the case of *Harman and Hewitt,*[125] and in order to anticipate its final adverse decision that was handed down ten days after the Act was passed.[126] In the 1996 appeal of *R v Khan*,[127] Lord Nolan described the continuing lack of a statutory scheme regulating the use of surveillance devices by the police as 'astonishing', and it was the prospect of a subsequent adverse ruling by the ECtHR in Khan's case under Article 8 that gave rise to Part III of the Police Act 1997. And it was the Strasbourg Court's 1997 adverse ruling in *Halford v United Kingdom* that led to the enactment of RIPA in 2000.[128]

51. The right to privacy – or, more accurately, *respect* for privacy[129] – under Article 8 in fact involves a number of different constituent rights and principles. First of all, Article 8(1) protects not only a person's

---

122. Originally Art 53 but now Art 46(1).
123. Section 2 of the HRA requires the courts to 'take into account' the decisions of the ECHR; section 3 directs courts to interpret legislation consistently with Convention rights 'so far as it is possible to do so', and section 4 allows the courts to declare legislation incompatible with Convention rights (although declarations do not affect the validity or continuing effect of the provision in question). Lastly, S 6 makes it unlawful for any public body (including government ministers and the courts) to act incompatibly with Convention rights save to the extent that they are required to do so by legislation.
124. *Malone v United Kingdom* (1984) 7 EHRR 14.
125. (1992) 14 EHRR 657.
126. The Security Service Act 1989 received royal assent on 27 April 1989. In a report dated 9 May 1989, the Commission held that the 'existence of practices in the UK permitting secret surveillance', the fact that the applicants were subjects of surveillance, and the lack of a legal framework governing the use of surveillance powers breached Art 8(2).
127. [1996] UKHL 14.
128. *Halford v United Kingdom* (1997) 24 EHRR 523.
129. Whether the attenuated formulation 'right to respect for' privacy adds or takes anything away from the more direct 'right to privacy' has been much debated over the years: see eg, Harris, O'Boyle and Warbrick, *Law of the European Convention on Human Rights*, 2nd ed (OUP: 2009), pp381-385.

'private life' but also his or her 'home' and 'correspondence'. These are separate concepts but obviously capable of considerable overlap: so, for example, a bug planted in someone's kitchen would engage both their right to their home but also their private life, while the interception of someone's mobile phone call made from a crowded street would engage the right to respect for their private life but also their 'correspondence' (not to mention those of the person at the other end of the phone call).

52. Indeed, the concept of 'private life' under Article 8 is a wide one, and not restricted to activities in the living room or bedroom. As the Strasbourg Court said in the case of *PG and JH v United Kingdom*,[130] 'private life' is 'a broad term not susceptible to exhaustive definition', and includes not only such obviously personal information such as 'gender identification, name and sexual orientation and sexual life' but also 'a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world', including 'activities of a professional or business nature'. It referred to a 'zone of interaction' that a person might have in their dealings with others, '*even in a public context*, which may fall within the scope of 'private life'' under Article 8.[131]

53. So, for example, the concept of 'private life' has been held to apply to covert interception of calls made to and from a person's place of work,[132] CCTV surveillance of a person attempting suicide late at night on Brentwood high street,[133] and the surreptitious police recording of conversations of two suspects while held in a police cell.[134] The terms 'home' and 'correspondence' have similarly broad meanings: the former has been held to include, for example, a person's caravan,[135] a home office,[136] and a hotel room used by a homeless person,[137] while the latter now extends beyond ordinary post to include phone calls,[138] pager messages,[139] emails and general Internet usage.[140]

54. Second, the substantive rights under Article 8(1) are subject to the provisions of Article 8(2), which permit considerable interference by the state with a person's privacy for the sake of a wide range of interests, including national security, public safety, the prevention of disorder or crime and the protection of the rights and freedoms of others. In common with other qualified rights under the Convention, however, interference with privacy must be: i) 'in accordance with the law'; ii) for the sake of one of the legitimate aims identified in Article 8(2); and iii) 'necessary in a democratic society', ie, proportionate and rationally connected to the aim in question. Most of the UK cases

130. *PG and JH v United Kingdom* [2001] ECHR 546 at para 56.
131. Ibid. Emphasis added.
132. See eg, *Halford v UK* (1997) 24 EHRR 523 at para 44: 'it is clear from its case-law that telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence' within the meaning of Art 8(1)'; and *Kopp v Switzerland* (1999) 27 EHRR 91 at para 50.
133. *Peck v United Kingdom* (2003) 36 EHRR 41 at para 59: 'The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life ... On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations'.
134. Notably, though, it was not the contemporaneous monitoring of the conversations by police that engaged Art 8 so much as the *recording* of the suspects' conversations: see *PG and JH*, n130 above, at para 59: 'While it is generally the case that the recordings were made for the purpose of using the content of the conversations in some way, the Court is not persuaded that recordings taken for use as voice samples can be regarded as falling outside the scope of the protection afforded by Art 8. A permanent record has nonetheless been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data. Though it is true that when being charged the applicants answered formal questions in a place where police officers were listening to them, the recording and analysis of their voices on this occasion must still be regarded as concerning the processing of personal data about the applicants'.
135. See eg, *Buckley v United Kingdom* (1996) 23 EHRR 101 at para 54 and *Connors v United Kingdom* (2004) 40 EHRR 189 at para 58.
136. See eg, *Niemetz v Germany* (1992) 16 EHRR 97 at para 30.
137. *O'Rourke v United Kingdom* (App no. 39022/97, admissibility decision), although the Court expressed 'significant doubts' as to whether 'the applicant's links with the hotel room were sufficient and continuous enough to make it his 'home' at the time of his eviction'.
138. See *Klass v Germany* (1978) 2 EHRR 214, para 41.
139. See eg, *Taylor–Sabori v United Kingdom* (2003) 36 EHRR 17.
140. See eg, *Copland v United Kingdom* (App no. 62617/00, 3 April 2007).

involving surveillance have focused on the first requirement of Article 8: the requirement that any interference with privacy must be 'in accordance with law', ie, have a legal basis, be sufficiently clear and precise, together with adequate safeguards against abuse. As we will see below, however, the necessity and proportionality of particular surveillance measures tends not to be the subject of detailed consideration by the ECtHR for a variety of reasons.

'In accordance with the law'

55. Article 8(2) requires that any interference with privacy must be 'in accordance with the law'. What this means in substance is contained in a series of principles that have been developed over time in a series of cases by the ECHR. In outline, these principles are that any surveillance activity by a public body must be:

    i. authorised by legislation;

    ii. the relevant law must be sufficiently clear and precise; and

    iii. contain adequate and effective safeguards against abuse.

56. The need for these requirements was set out by the Court in its 1978 decision of *Klass v Germany*,[141] the first major Strasbourg case to deal with surveillance powers. The Court began by noting that, by its very nature, covert surveillance made it extremely difficult for a person to know whether his or her privacy was being interfered with:[142]

> where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8, or even to be deprived of the right granted by that Article, without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions … *The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be … removed by the simple fact that the person concerned is kept unaware of its violation.*

57. This led the Court to conclude that the 'mere existence' of secret surveillance powers gave rise to 'a menace of surveillance' that amounted to an interference with the privacy of *any* person who might potentially be subject to it:[143]

> this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for private and family life and for correspondence

141. (1978) 2 EHRR 214.
142. Ibid, para 36. Emphasis added.
143. Ibid, para 41.

Accordingly, the Court concluded, 'powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions'.[144]

58. In its subsequent decision in *Malone v United Kingdom*, the Strasbourg Court made clear that the requirement of 'in accordance with law' under Article 8 did not mean merely that there had to be some legal basis for the exercise of surveillance powers. In *Malone*, the Court considered the then-UK law governing interception of communications, which was carried out under warrant by the Home Secretary but with no corresponding basis in either common law or statute.[145] The ECtHR held that, although the usual requirements of legal certainty under Article 8(2) could not be expected in the field of surveillance, given the need to preserve secrecy:[146]

> Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

In particular, since the covert nature of surveillance meant that it was not open to 'scrutiny by the individuals concerned or the public at large', it was especially important for legislation to restrict the scope of any discretion afforded to officials:[147]

> it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, *the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.*

59. In *Malone*, the Strasbourg Court found that the wholesale absence of any statutory scheme governing the interception of communications by police meant that it could not 'be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive'.[148] This failure of English law to 'indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities', the Court held, breached Article 8 because 'the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking'.[149]

60. As noted earlier, the Court's decision in *Malone* was just the first in a series of adverse rulings against the UK because of the lack of any proper statutory footing for its exercise of various surveillance powers; rulings that – in turn – prompted a series of legislative changes. So, for example, *Malone* led to the passing of the Interception of Communications Act 1985, which laid down a detailed statutory scheme governing the interception of communications by law enforcement and intelligence services - albeit only on public communications networks. And when the Assistant Chief Constable of Merseyside Police, Mrs Halford, complained that the 1985 Act did not apply to interception of her

144. Ibid, para 42. See also para 49: 'The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate'.
145. Save for the exceedingly general provisions of para 1(1) of Schedule 5 of the Post Office Act 1969.
146. *Malone*, n124 above, para 67.
147. Ibid, para 68. Emphasis added.
148. Ibid, para 79.
149. Ibid.

phone calls on Merseyside Police's *internal* phone system – a *private* communications network – the ECtHR ruled that the failure of the law to regulate this kind of interference breached Article 8(2) 'since the domestic law did not provide adequate protection to Ms Halford against interferences by the police with her right to respect for her private life and correspondence'.[150] *Halford*, in turn, became one of the reasons for replacing the 1985 Act with RIPA in 2000.[151] Similarly, in its judgment in the 2000 case of *Khan*, the Strasbourg Court held that the lack of any 'domestic law regulating the use of covert listening devices' meant that the consequent interference with privacy was not 'in accordance with the law' under Article 8(2).[152] As noted earlier, by the time of the Court's decision in *Khan*, the Police Act 1997 had already been passed in anticipation of its ruling.

61. Much of the Court's rulings on the 'accordance with the law' point in surveillance cases have focused on the level of foreseeability that the legislation must provide. In *Malone and Khan,* for instance, the test was whether the law was 'sufficiently clear' as to give those subject to it an 'adequate indication' as to when authorities could use such powers.[153] In a Swedish case concerning information held in a person's secret police file that was used to refuse him security clearance in a Naval Museum,[154] however, the Court held that the requirement of foreseeability did *not* mean that a person should be able 'to foresee precisely' what checks the police might make against his file for the purposes of national security. Similarly, in the 1994 admissibility decision of *Christie*,[155] the European Commission rejected a complaint from a trade unionist that the interception of his overseas communications by GCHQ breached Article 8. In particular, the Commission rejected the submission that 'national security' as a grounds of interception provided by the 1985 Act was overbroad and not subject to 'adversarial input which forms part of the judicial process of interpretation'. The Commission held it was enough for the purposes of the foreseeability requirement under Article 8(2) that such apparently 'general and unlimited' terms were 'explained by administrative or executive statements and instructions'. In the 2008 judgment of *Liberty and others v United Kingdom*,[156] however, the ECtHR held that the broad-based provisions of the 1985 Act which enabled so-called 'strategic' or large-scale interception of overseas communications in fact breached Article 8.[157] In particular, the Court noted:[158]

> The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other. The Court's approach to the foreseeability requirement in this field has … evolved since the Commission considered the United Kingdom's surveillance scheme in its above-cited decision in Christie v. the United Kingdom.

150. *Halford*, n128 above, para 52. See also paras 49-52: 'the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures ... The Court notes that the 1985 Act does not apply to internal communications systems operated by public authorities ... and that there is no other provision in domestic law to regulate interceptions of telephone calls made on such systems ... It cannot therefore be said that the interference was 'in accordance with the law' for the purposes of Art 8(2) of the Convention'.
151. The inadequacy of the 1985 Act was further confirmed in *Liberty and others v United Kingdom* (App No 58243/00, 1 July 2008).
152. *Khan v United Kingdom* (2001) 31 EHRR 1016, paras 26-27.
153. *Malone,* n124 above, para 67 and *Khan,* ibid, para 26.
154. *Leander v Sweden* (1987) 9 EHRR 433 at para 51.
155. *Christie v United Kingdom* (App no. 21482/93, 27 June 1994).
156. See n151 above.
157. *Liberty and others*, n151 above, para 69: 'the Court does not consider that the domestic law at the relevant time [the 1985 Act] indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. *In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material*'. Emphasis added.
158. Ibid, para 63.

The Court has also stressed on a number of occasions the need for 'clear, detailed rules' governing interception of telephone conversations, 'especially as the technology available for use is continually becoming more sophisticated'.[159]

62. The third aspect of the 'in accordance with the law requirement' is the need for 'adequate and effective safeguards against abuse'.[160] What constitutes adequate safeguards will depend on the particular type of surveillance involved, eg, interception of communications, audio or video surveillance inside a person's home, or simply the recording and storage of personal information in a police or intelligence database. So, for example, in relation to interception of communications, the Strasbourg Court has said:[161]

> In its case-law on secret measures of surveillance, the Court has developed the *following minimum safeguards that should be set out in statute law in order to avoid abuses of power:* the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed…

63. The importance of oversight – in particular, *judicial* oversight – as a safeguard has been a central feature of the Strasbourg case-law on surveillance powers. In *Klass*, the Court noted that the need to keep surveillance activities secret from the individual being surveilled meant that it was all the more important to provide internal oversight to prevent abuse by public authorities:[162]

> One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention … *The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.*

In *Klass,* however, the Strasbourg Court stopped short of stating that judicial oversight was required in every case. In the German legislation in question, initial decisions were taken by an 'official qualified for judicial office', with subsequent oversight being provided by a parliamentary board and commission.[163] Although the Court noted that, given the obvious potential for abuse of secret powers and the insidious consequences, 'it is in principle desirable to entrust supervisory control to a judge', it was nonetheless satisfied that the parliamentary board and commission were sufficiently 'independent of the authorities carrying out the surveillance' to be able to give 'an objective

159. See eg, *Kruslin v France* (1990)12 EHRR 547, para 33; *Kopp v Switzerland* (1998) 27 EHRR 91, para 72; *Weber and Savaria v Germany* (application no 54934/00, 29 June 2006), para 75; *Liberty and others,* ibid, para 62.
160. See eg, *Klass*, n138 above, para 50: 'This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law'.
161. *Weber & Savaria v Germany*, n159 above, para 95.
162. *Klass*, n138 above, para 55, emphasis added.
163. Ibid, para 56.

ruling'.[164] Significantly, in a separate complaint made by the applicant in *Klass* under Article 6 – the right to a fair trial – the Court held that:[165]

> As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6; as a consequence, it of necessity escapes the requirements of that Article.

In other words, the Court held that since there was no way a person subject to secret surveillance could know that he or she was being surveilled, it was, therefore, impossible for the oversight procedure to meet the basic requirements of procedural fairness. Surprisingly, in a recent judgment, *Kennedy v United Kingdom*,[166] the ECtHR held that the procedures of the IPT under Part 4 of RIPA were not incompatible with Article 6 despite the fact that they involved no right of the applicant to know the evidence on the other side. The shortcomings of the Court's decision in *Kennedy* will be examined in detail in Chapter 9 below.

For a legitimate aim

64. Article 8(2) sets out a number of grounds on which public bodies may interfere with the right to privacy under Article 8(1). In order for any interference to be justified under Article 8(2), a state must, therefore, show that the interference falls within one of the legitimate aims listed. These grounds are extremely broad, however (see eg, 'the economic well-being of the country'), and the requirement to show a legitimate aim is rarely a steep hurdle for a state to meet. This is especially true in the case of surveillance powers: because the focus of the Court tends to be the legal framework for the exercise of surveillance powers rather than the specific surveillance measures adopted in a particular case, it is relatively easy for states to point to one or more of the general justifications for surveillance powers – the obvious ones being the prevention of disorder or crime; public safety; national security; and the protection of the rights and freedoms of others. See, for example, the Court's analysis in *Leander v Sweden*:[167]

> The aim of the Swedish personnel control system is clearly a legitimate one for the purposes of Article 8, namely the protection of national security.

In most cases of qualified rights, the real question is not whether a given interference is for a legitimate aim but whether the particular measure is necessary and proportionate to the aim pursued. As we will see in a moment, though, this is something that arises for consideration only infrequently in cases involving surveillance powers.

'Necessary in a democratic society'

65. The principle that any interference with a qualified right such as Article 8 must be 'necessary in a democratic society' is one of the core principles of human rights law. In general, it means that

164. Ibid.
165. Ibid, para 75.
166. App no. 26839/05 18 May 2010.
167. See n154 above, para 49.

a state must not only demonstrate that its interference with a person's right meets a 'pressing social need' but also that it is '*proportionate* to the legitimate aim pursued'.[168] When assessing the necessity and proportionality of a state's measures, the Court typically affords the state a 'margin of appreciation', the breadth of which depends on a number of factors including the aim in question. In *Leander*, for instance, the Court noted that:[169]

> national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life.

In Leander's own case, the Court found that his legitimate interest in working for the Naval Museum was outweighed by the state's interest in using sensitive intelligence material 'when assessing the suitability of candidates for employment in posts of importance for national security'.[170] In *Peck v United Kingdom*, the Court again acknowledged that states enjoyed a margin of appreciation:[171]

> In cases concerning the disclosure of personal data, the Court has recognised that a margin of appreciation should be left to the competent national authorities in striking a fair balance between the relevant conflicting public and private interests. *However, this margin goes hand in hand with European supervision …* and the scope of this margin depends on such factors as the nature and seriousness of the interests at stake and the gravity of the interference.

In Peck's case, however, the balancing of interests was not national security but rather the public interest in detecting and preventing of crime, which was the general justification for Brentwood Borough Council's operation of its CCTV system. Peck had been caught on CCTV late at night attempting suicide on Brentwood High Street and the CCTV operator had alerted the local police, leading to his being taken into custody. Peck did not challenge the Council's use of CCTV – which had ultimately helped him – but rather the Council's subsequent decision to release footage of the incident to the media, including national television, causing him considerable distress. Although it was not disputed that CCTV played 'an important role' in 'preventing and detecting crime', Peck himself was 'not charged with, much less convicted of, an offence'.[172] The Court held that the Council's failure to take steps to either seek Peck's consent before disclosing the footage or, alternatively, ensure that he could not be identified from the footage, meant that the interference with Peck's private life was disproportionate and hence breached Article 8.[173]

66. Most recently, in the case of *Uzun v Germany*,[174] the Strasbourg Court considered the proportionality of GPS surveillance of a member of a splinter group of the Red Army Faction suspected of

168. See eg, *Olsson v Sweden* (1988) 11 EHRR 259 at para 67. Emphasis added.
169. *Leander*, n154 above, para 59.
170. Ibid. The Court went on to note that although 'the contested interference adversely affected Mr. Leander's legitimate interests through the consequences it had on his possibilities of access to certain sensitive posts within the public service. On the other hand, t*he right of access to public service is not as such enshrined in the Convention ... and, apart from those consequences, the interference did not constitute an obstacle to his leading a private life of his own choosing'* [emphasis added] (ibid).
171. *Peck*, n133 above, para 77. Emphasis added.
172. Ibid, para 79.
173. Ibid, para 87.
174. *Uzun v Germany* (App no.35623/05, 2 September 2010).

involvement in a bombing campaign. In Uzun's case, a GPS tracking device was secretly attached to his associate's car after other surveillance measures had proved unsuccessful. In view of the seriousness of the offences being investigated, the relatively short period of time the surveillance was carried out (roughly three months) and the fact that the authorities had already tried less intrusive means, the Court held that the use of GPS tracking was proportionate.[175]

67. However, the assessments of proportionality in the cases of *Leander*, *Peck* and *Uzun* are unusual for surveillance cases, due largely to the Strasbourg Court's own case-law which permits states to keep secret the very fact of surveillance in most cases. In a number of common law countries, for instance, subjects of surveillance are required by law to be notified so that they may bring an ex post facto challenge to the original decision of the authorities to put them under surveillance. In *Klass*, however, the Court agreed with the German government's submission that a general requirement of post-surveillance notification would tend to undermine its operational effectiveness.[176] As noted above, the Court was quick to appreciate the danger of surveillance decisions that were effectively 'unchallengeable' because a person could be deprived of their right to privacy without ever being aware of it.[177] This, in turn, led the Court to place particular emphasis on the 'accordance with the law' requirements of Article 8(2), in particular the need for adequate and effective safeguards against abuse, particularly in relation to oversight:[178]

> Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. *Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights.*

68. What this means in practice, however, is that it will be almost impossible for an individual to gainsay the necessity and proportionality of a surveillance decision; first, because they will only very rarely be *aware* that one has been made; and second, because they will in any event not be permitted to *know the basis* on which it has been made. As the Court said in *Klass*, secret surveillance decisions are effectively non-justiciable, at least as far as the person affected is concerned.[179] This has several consequences. First, it means that any evidence supporting the decision is not tested to adversarial challenge in the usual way. Second, it means that surveillance decisions almost entirely escape the scrutiny of ordinary courts, at least until a further decision is made to use the fruits of that surveillance in evidence. Third, it means that surveillance decisions also escape broader public

175. Ibid, para 80.
176. *Klass*, n138 above, para 58: 'In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. *Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore ... such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents*. In the Court's view, in so far as the 'interference' resulting from the contested legislation is in principle justified under Art 8(2) ... the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the 'interference'. Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction' [emphasis added].
177. See *Klass*, n138 above, para 36.
178. Ibid, para 55. Emphasis added.
179. Ibid, para 75.

scrutiny, leaving the public unable to assess whether the law is being applied properly. Fourth, and most obviously, it is fundamentally unjust that individuals should be deprived of the protection of an essential component of their right to privacy under Article 8. This basic unfairness can only be offset, as the Court noted in *Klass*, by the provision of 'adequate and equivalent guarantees' in the surveillance legislation itself. As we will see, however, the great majority of surveillance decisions under RIPA over the past decade have been made without proper judicial oversight or control.

Chapter 3
Interception of communications

69. The practice of secretly intercepting communications for law enforcement and intelligence purposes is an extremely old one. As the Birkett Report noted in 1957,[180] the first public reference to the Secretary of State authorising the opening of letters under warrant was in 1663; President Lincoln apparently authorised the tapping of telegraphs during the American Civil War and in its 1984 decision in the *Malone* case, the ECtHR noted that 'the power to intercept telephone messages has been exercised in England and Wales from time to time since the introduction of the telephone'.[181] However, as Sir Robert Megarry VC noted in his 1979 ruling in the same case, there was for many years no statutory basis for the Home Secretary's use of interception warrants:[182]

> This case seems to me to make it plain that telephone-tapping is a subject which cries out for legislation … However much the protection of the public against crime demands that in proper cases the police should have the assistance of telephone tapping, *I would have thought that in any civilised system of law the claims of liberty and justice would require that telephone users should have effective and independent safeguards against possible abuses.* The fact that a telephone user is suspected of crime increases rather than diminishes this requirement: suspicions, however reasonably held, may sometimes prove to be wholly unfounded.

70. Despite Megarry's plea, the Home Secretary Willie Whitelaw told Parliament in 1980 that the government had no plans to introduce legislation on the issue:[183]

> The interception of communications is, by definition, a practice that depends for its effectiveness and value upon being carried out in secret and cannot, therefore, be subject to the normal processes of parliamentary control. Its acceptability in a democratic society depends on its being subject to ministerial control *and on the readiness of the public and their representatives in Parliament to repose their trust in the Ministers concerned to exercise that control responsibly* and with a right sense of balance between the value of interception as a means of protecting order and security and the threat which it may present to the liberty of the subject.

---

180. *Report of the Privy Councillors appointed to inquire into the interception of communications* (Cmnd 283, October 1957).
181. (1984) 7 EHRR 14 at para 28.
182. *Malone v Metropolitan Police Commissioner* [1979] 344 Ch at 380-381, emphasis added.
183. HC Debates col 207, 1 April 1980. Emphasis added.

> Within the necessary limits of secrecy, I and my right hon. Friends who are concerned are responsible to Parliament for our stewardship in this sphere. There would be no more sense in making such secret matters justiciable than there would be in my being obliged to reveal them in the House. *If the power to intercept were to be regulated by statute, the courts would have power to inquire into the matter and to do so, if not publicly, at least in the presence of the complainant. This must surely limit the use of interception as a tool of investigation.* The Government have come to the clear conclusion that the procedures, conditions and safeguards described in the Command Paper ensure strict control of interception by Ministers, are a good and sufficient protection for the liberty of the subject, and would not be made significantly more effective for that purpose by being embodied in legislation. The Government have accordingly decided not to introduce legislation on these matters.

As noted above, the government was eventually prompted to shift its position by the adverse ruling of the ECtHR in *Malone* in 1984, which led to the Interception of Communications Act 1985. This established the use of interception warrants made by the Secretary of State,[184] the office of the Interception of Communications Commissioner to review the Secretary of State's exercise of his power to make warrants,[185] and the Interception of Communications Tribunal to hear complaints concerning interceptions.[186]

71. The 1985 Act only applied to communications sent by post or 'public telecommunications systems', however, and not to such private systems as the internal phone network of an office. This led the Strasbourg Court to again find the UK in breach of Article 8 in its 1997 ruling in Halford.[187] This, in turn, led the government to publish its 1999 White Paper which proposed fresh legislation to deal with both interception of communications and communications data.[188] This was overtaken, however, by proposals to establish a broader statutory framework governing surveillance powers as a whole, ie, RIPA 2000.

72. The covert interception of communications by law enforcement and intelligence bodies is now governed, therefore, by Part I of RIPA.

73. Section 1 of the Act makes it a criminal offence for any person to intentionally intercept communications 'without lawful authority'. In most cases, 'lawful authority' means a warrant issued by the Secretary of State under section 5 (the Home Secretary in respect of England and Wales, the Scottish Executive in relation to Scotland, the Northern Ireland Secretary in respect of Northern Ireland, or the Foreign Secretary in relation to interceptions of overseas communications). However, sections 3 and 4 of RIPA set out a limited number of circumstances in which interception is lawful without a warrant, including:

    a. where *both parties* either consent or are 'reasonably believed' to consent;[189]

    b. where *one party* consents to the interception (eg, one party is recording the conversation without the other's knowledge – sometimes referred to as 'participant monitoring')[190] *and* the

184. Sections 2-5.
185. Section 8.
186. Section 7.
187. See n128 above.
188. *Interception of Communications in the United Kingdom* (June 1999, Cm 4368).
189. Section 3(1).
190. See eg, *Regina v X* [2004] EWCA Crim 1243 at para 18 per Hughes J.

interception has been authorised as directed surveillance (see Chapter 6 below) rather than an interception;[191]

c. where the interception takes place on a *private* telecommunications network (eg, an office's internal phone system) with the *consent* of the controller of the system (eg, the employer);[192] or

d. where the communications are made *to or from a prison or psychiatric hospital*.[193]

74. An interception warrant may target either: i) a single person; or ii) a single set of premises.[194] Once made, all the communications of that person or premises may be lawfully intercepted. In the case of a person, that would include their mobile phone, landlines, fax numbers, email and ISP accounts, and any post addressed to them at any location. In the case of a set of premises, it would cover all the communications to and from that address. So if an office has 100 people working in it, for example, each with their own computer and direct line, a single interception warrant would be enough to cover all their phone and email traffic. In this way, merely publishing the number of interception warrants issued in a year is likely to give a highly misleading impression of the true extent of interceptions, since a single warrant may cover all the communications of an entire workplace.

75. Unlike some other kinds of surveillance under RIPA, only a relatively narrow class of law enforcement and intelligence agencies may apply to the Secretary of State for an interception warrant to be issued, specifically the Metropolitan Police and its counterparts in Scotland and Northern Ireland, MI5, MI6, GCHQ, HM Revenue & Customs, the Serious Organised Crime Agency, the Scottish Crime and Drug Enforcement Agency, and the Ministry of Defence's Defence Intelligence unit.[195]

76. In order for a warrant to be issued, the relevant Secretary of State must be satisfied that it is necessary either:[196]

a. in the interests of national security;

b. for the purpose of preventing or detecting serious crime; or

c. for the purpose of safeguarding the economic well-being of the United Kingdom.[197]

He or she must also be satisfied that 'the conduct authorised by the warrant is *proportionate* to what is sought to be achieved by that conduct'.[198] In other words, the assessment of whether the interference with privacy posed by an interception warrant is necessary and proportionate under Article 8(2) is made in the first instance by a government minister.

---

191. Sections 3(2) and 48(4).
192. Sections 1(6) and 3(3).
193. Sections 4(4)-4(6).
194. Section 8(1).
195. Section 6(1).
196. Section 5(2)(a) and (3). The Secretary of State may also make interception warrants in relation to criminal investigations for the purposes of international mutual assistance agreements, eg, if the French government requests the UK government's assistance in investigating serious organised crime, etc.
197. Section 5(5) further provides that, in order to be necessary for the sake of safeguarding the UK's economic well-being, an interception warrant must be aimed at obtaining 'information relating to the acts or intentions of persons outside the British Islands'.
198. Section 5(2)(b). Emphasis added.

77. Oversight of interception warrants is provided by the Interception of Communications Commissioner ('Interception Commissioner'), who is required by RIPA to be someone who 'holds or has held high judicial office'.[199] Indeed, some of the UK's most senior judges have previously held the post of Interception Commissioner including Lord Bingham, Lord Diplock, and Lord Nolan. The current Commissioner is Sir Paul Kennedy, a retired Court of Appeal judge. The Commissioner is required to 'keep under review' the issue of interception warrants by the Secretary of State,[200] as well as the work of the various agencies when applying for and carrying out interception warrants. He also has oversight of requests for communications data under Chapter 2 of Part 1 of RIPA (see Chapter 4).

78. Notably, however, the Commissioner has no power to review the making of regulations by the Secretary of State under Part I,[201] nor does his remit formally extend to the various circumstances in which interceptions may be made under Part 1 without a warrant.[202] This includes an unknown but plainly considerable number of interceptions that are carried out by the Prison Service.[203] In 2001, therefore, the Interception Commissioner agreed to undertake non-statutory oversight of interceptions of communications to and from prisons.[204] However, there continues to be no statutory oversight for any of the other circumstances in which interceptions may be carried out without a warrant, and in September 2010 the European Commission referred the UK government to the Court of Justice for the European Union due to, among other things, its continuing failure to provide full statutory oversight for interception of communications.[205] This is discussed in greater detail below.

79. Since Part 1 of RIPA came into force in October 2000,[206] more than 20,000 interception warrants have been issued by the Home Secretary and the Scottish Executive.[207] These figures do not include the total number of interception warrants made by the Northern Ireland Secretary or the Foreign Secretary, however, which remain unknown. This compares with a total of 12,799 warrants issued between 1990 and 1999, and only 4,641 warrants issued between 1980 and 1989.[208] As noted earlier,[209] the number of warrants issued also does not necessarily reflect the actual volume of communications that have been intercepted as a single warrant under RIPA may cover all communications to and from a single premises occupied by hundreds of people.

---

199. Section 57(5).
200. Section 57(2).
201. Section 57(4).
202. See Section 57(2). As the current Interception Commissioner notes, interception of prisoners' communications 'is mandatory in some cases, for example in relation to High Risk Category A prisoners and prisoners who have been put on the Escape List' (See *Report of the Interception of Communications Commissioner for 2010* (HC 1239, June 2011), para 8.4).
203. For instance, the 2009 report of the Interception Commissioner makes reference to 'one establishment in the High Security Estate' that 'decided that the telephone calls and correspondence of 476 prisoners needed to be monitored' (Sir Paul Kennedy, *Report of the Interception of Communications Commissioner for 2009* (HC 341, July 2010), para 4.10). Although this was criticised by the Commissioner as 'completely unrealistic and unattainable', it indicates the potential volume of communications that may be intercepted in a single unit. As of September 2011, there are currently more than 134 prisons in the HM Prison establishment, with a total adult prison population of 87,120 (Ministry of Justice monthly figures).
204. See Sir Swinton Thomas, *Report of the Interception of Communications Commissioner for 2001* (HC 1243, October 2002), para 59: 'I have been asked by the Home Office, and have agreed in principle, to oversee the interception of communications in prisons'.
205. See eg, 'Commission refers UK to court over privacy and personal data protection', EU Commission press statement, 30 September 2010 (IP/10/1215).
206. For the commencement date of Part 1 of RIPA, see para 3 of The Regulation of Investigatory Powers Act 2000 (Commencement No 1 and Transitional Provisions) Order 2000 (SI 200/2543).
207. The total number of interception warrants between 2000 and 2010 for England, Wales and Scotland is 20,237 (source: annual reports of the Interception of Communications Commissioner from 2000-2010). However, the figure given for the year 2000 does not distinguish between interception warrants issued under RIPA from October onwards and warrants issued under the previous 1985 Act up until the end of September.
208. Again, these are the warrants issued by the Home Secretary and Scottish Secretary only, and do not include interception warrants issued for Northern Ireland or overseas.
209. See n194 above.

Lack of prior judicial authorisation

80. As we saw in the previous chapter, the inevitable need to keep surveillance – and decisions about surveillance – secret gives rise to a serious protection gap because: i) people who are the subject of surveillance activities will not generally be aware that their privacy is being interfered with; and ii) even if they are, they will rarely be in a position to gainsay the necessity and proportionality of that surveillance. As the ECtHR has made clear, this makes it all the more important that the legal framework governing the exercise of surveillance powers provides 'adequate and effective safeguards' against abuse, including the possibility that a particular surveillance decision will be disproportionate.

81. The most obvious failing of Part 1 of RIPA, therefore, is the fact that applications for interception warrants are decided by a government minister rather than a judge. To put it another way, the ultimate assessment of whether it is necessary and proportionate to intercept someone's phone calls and emails is not made by an independent judicial authority but by the government minister responsible for the agency seeking to carry out the interception. When he introduced RIPA at its Second Reading in the House of Commons, however, the Home Secretary Jack Straw dismissed concerns about the lack of prior judicial authorisation for interception warrants:[210]

> The initial decision is made by a Secretary of State. It is a matter of practice and convenience, but not in any sense a diminution of people's human rights, that this country has that system. It works. There has been no overwhelming argument, or no substantial argument to change it. *If one looks at the practice in other countries, it does not necessarily follow that, just because a judicial warrant is required, there is a greater safeguard for the individual.* Indeed, I suggest that, in quite a number of other countries, the fact that a judicial warrant is required lessens the protection that is offered to people because the judicial warrant acts as a fig leaf for people's human rights, and not as a serious safeguard.

82. Unfortunately the Home Secretary did not provide any evidence to support his claim that judge-made warrants in other countries were a 'fig leaf' and 'not … a serious safeguard'. Straw did point out, though, that the process of interception under RIPA was 'also subject to extensive judicial scrutiny – albeit retrospectively'.[211] Whether this retrospective judicial scrutiny is adequate is something that we will consider in the next section. The role of the Home Secretary has been vigorously defended, however, by successive Interception Commissioners – in many cases using identical language, year after year. In his 2003 report, for instance, the then-Commissioner Sir Swinton Thomas wrote:[212]

> Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity or proportionality are not met, and the agencies are well aware that the Secretary of State does not act as a 'rubber stamp'.

---

210. Hansard, HC Debates col 770, 6 March 2000. Emphasis added.
211. Hansard, HC Debates col 768, 6 March 2000.
212. Swinton Thomas, *Report of the Interception of Communications Commissioner for 2003* (HC 883, July 2004), para 8.

In 2010, by contrast, his successor Sir Paul Kennedy wrote:[213]

> Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity or proportionality are not met, and the agencies are well aware that the Secretary of State does not act as a 'rubber stamp'.

Sadly, the reliance of successive Interception Commissioners upon such boilerplate language does little to inspire confidence in their findings. In his most recent report, though, Sir Paul broke with several years of tradition to produce some fresh text on the subject:[214]

> The outright refusal of an application is rare, mainly because an authorisation request *crosses the desks of a number of officials and, in certain circumstances, legal advisers and is scrutinised with some considerable care before it reaches the Secretary of State or the Scottish Minister.* A final comment recommending signature or highlighting risks is made by someone at Senior Official or Director Level in, for example, the Home Office or Foreign Office prior to submission to the relevant Secretary of State or Scottish Minister. Overall I am confident that, as the agencies are aware, the Secretary of State and the Scottish Ministers are not simply 'rubber-stamping' requests presented to them.

83. The Interception Commissioner presents the role played by the relevant Secretary of State as a diligent one. It is also worth recalling the findings of the ECtHR in *Klass* that executive oversight of interceptions could be an adequate safeguard where the supervisory body was sufficiently 'independent of the authorities carrying out the surveillance' to give 'an objective ruling'.[215]

84. However, there are at least two serious problems with the role of the Secretary of State under Part 1 of RIPA (and, to an extent, some of the Court's reasoning in *Klass*). First, it is well-known that all government ministers rely to a significant extent upon the advice of their officials when carrying out their functions, something which was highlighted by Sir Paul's reference to the number of desks which an authorisation request has to cross before it reaches the relevant Secretary of State. The diligence of the Home Secretary when considering whether to grant an interception warrant is not generally in doubt, but it is not a qualification for her office that she herself possess any expertise in either surveillance, criminal investigation, intelligence-gathering or human rights law. Even in *Klass*, by contrast, the initial interception decision was taken by 'an official qualified for judicial office'.[216] It follows from this that any expertise that the Secretary of State does have access to when deciding whether to grant a warrant must come from the same officials whose application she is meant to be objectively considering. Sir Paul's reference to 'legal advisers', for instance, will be government lawyers and, in the case of the Home Secretary, the Home Office Legal Adviser's Branch – those lawyers tasked with helping to defend her decisions and, not incidentally, the same lawyers who advised on the compatibility of RIPA with Article 8 to begin with. The Interception Commissioners have cited the occasional refusal as evidence that the Secretary of State does not act as a rubber stamp, but no actual figures have ever been given for the number of 'outright and final' refusals –

213. Kennedy, n203 above, para 2.3.
214. Kennedy, *Report of the Interception of Communications Commissioner for 2010* (HC 1239, June 2011), para 2.4. Emphasis added.
215. *Klass*, n138 above, para 56.
216. Ibid.

despite there being no obvious reason not to do so – which tends to suggest that the true number is very small indeed.

85. Second and more generally, it is also very well-known that the police and intelligence agencies are sometimes under enormous pressure to achieve results in the fight against terrorism and other serious crime and the same is no less true of the government ministers who are politically accountable for their activities. In such cases, a politician who is considering an application from the police or the intelligence services might well decide that it is better to grant an interception warrant she knows is disproportionate in the hopes of obtaining the results sought. She may even decide that the risk of subsequent criticism from the Interception Commissioner (assuming the warrant was one that he subsequently inspects)[217] would be preferable to the likely public outrage that would follow in the wake of a terrorist attack, for example. The last decade has shown that this is not an uncommon position for government ministers to adopt, particularly in relation to such controversial issues as counter-terrorism, criminal justice or immigration and asylum.[218] As Lord Dyson noted in relation to the secret policy for the blanket detention of foreign prisoners operated by the Home Office between 2006 and 2008, for instance:[219]

> It is material that there is no suggestion that officials acted for ulterior motives or out of malice towards the appellants. Nevertheless, there was a deliberate decision taken at the highest level to conceal the policy that was being applied and to apply a policy which, to put it at its lowest, the Secretary of State and her senior officials knew was vulnerable to legal challenge. *For political reasons, it was convenient to take a risk as to the lawfulness of the policy that was being applied and blame the courts if the policy was declared to be unlawful.*

If this is the approach that Home Office ministers were willing to take in relation to the detention of foreign prisoners in circumstances where judicial review was a real possibility, therefore, it hardly seems inconceivable that ministers might also adopt the same attitude in relation to interception decisions, especially where – for practical reasons – the likelihood of challenge is virtually nil. Not all government ministers have such a dubious attitude towards legality, of course, and all are ultimately accountable to the electorate for their decisions. But, as the foreign prisoner scandal shows, it is this very accountability that leads at least some of them to disregard the rights of unpopular minorities in favour of what they see as the broader public interest. The same mandate that gives elected officials their democratic legitimacy is what makes them so ill-placed to dispassionately assess the merits of intercepting someone's communications. And although some government ministers may be more diligent than others in this regard, privacy is too important a matter to be left to the lottery of a politician's integrity.

86. For these reasons, the sanguine assessments of the Interception Commissioner do little to dispel serious concerns about the granting of interception warrants. If the right to privacy is to be attended by 'adequate and sufficient' safeguards against unnecessary interference, then it is plainly

---

217. See page 6 below.
218. See eg, *Assessing Damage, Urging Action*: *Report of the Eminent Jurists Panel on Terrorism Counter-Terrorism and Human Rights* (February 2009).
219. *Walumba Lumba v Secretary of State for the Home Department* [2011] UKSC 12 at para 166. Emphasis added. See also eg, Baroness Hale at para 205: 'These are just the sort of circumstances, where both Ministers and their civil servants are under pressure to do what they may know to be wrong, in which the courts must be vigilant to ensure that their decisions are taken in accordance with the law. To borrow from the civil servants' correspondence, the courts must be prepared to take the hit even if they are not'.

desirable that the decision whether to issue an interception warrant should be made by a judge rather than a senior government minister. As the Court said in *Klass*:[220]

> The rule of law implies … that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, *judicial control offering the best guarantees of independence, impartiality and a proper procedure*.

87. Leaving aside the basic question of principle, the main objections to prior judicial authorisation of interception warrants appear to be operational in nature. Giving evidence to the Joint Committee on Human Rights in 2007, the outgoing Interception Commissioner Sir Swinton Thomas explained his own view:[221]

> From a practical point of view, which I suppose is what I am more concerned with, I think it is a very bad idea to put [interception decisions] in the hands of a judge. As things are at the moment, if you know that a bomb has been taken on a train in Leeds and is on its way to King's Cross and you need information, in a matter of minutes you can get a warrant to intercept the communications of that suspected terrorist. Likewise with a serious crime, if a very large consignment of class A drugs has arrived at Dover and is on its way up to Manchester, the Secretary of State is always on duty, 24 hours a day. It is very often absolutely vital that you act with as much speed as you possibly can. That is what currently happens. You can get a warrant or a modification, which is equally important, straight away. Going to a judge would not permit that degree of elasticity. If it is done by a judge, the other side must have the right to be heard and you will not be able to acquire a judicial hearing at the sort of speed that papers can be put in front of the Secretary of State.

88. There are three problems with Sir Swinton's complaint, however. First, his account of the speed and flexibility of the authorisation process is seriously at odds with his successor Sir Paul Kennedy's description of the same process, in particular his claim that each request crossed 'the desks of a number of officials and … is scrutinised with some considerable care'.[222] Second, Sir Swinton's objection overlooks the fact that judges issue warrants and orders in a great many urgent situations every day – including for instance search warrants, asset-freezing orders and even authorisations for intrusive surveillance under Part 2 of RIPA – without any obvious difficulty. As Lord Lloyd of Berwick – himself a former Interception Commissioner – said in the same evidence session, 'I do not believe there would be any great difficulty in getting [authorisation] almost as quickly with the Secretary of State'.[223] In most countries which require prior judicial authorisation for interceptions, for example, there is provision for emergency self-authorisation by police which must be confirmed by a judge within 24 or 48 hours. A similar procedure exists for authorisations for police to conduct intrusive surveillance under Part 2 of RIPA,[224] as we will see in Chapter 5. Third, Sir Swinton's claim that judicial authorisations would require 'the other side ... to be heard' is fanciful: there is no reason why applications for interception warrants would not be made in camera and ex parte, in

220. See n138 above. See also eg, *Dumitru Popescu v Romania (No 2)* (App No. 71525/01, 26 April 2007), paras 70-73 and *Iordachi and others v Romania* (App No. 25198/02, 10 February 2009), para 40: 'the body issuing authorisations for interception should be independent and ... there must be either judicial control or control by an independent body over the issuing body's activity'.
221. Evidence to the Joint Committee on Human Rights, 12 March 2007, Q26.
222. See n214 above.
223. Evidence to the Joint Committee on Human Rights, 12 March 2007, Q28.
224. Section 35 of RIPA.

the manner of search warrants or asset-freezing orders.[225] For this reason, the Joint Committee on Human Rights recommended that 'RIPA be amended to provide for judicial rather than ministerial authorisation of interceptions, or subsequent judicial authorisation in urgent cases'.[226]

89. In fact, the most plausible explanation for the government's resistance to judicial authorisation of interception warrants is neither democratic principle or concerns about operational delay but rather the tendency of the intelligence services to resist judicial scrutiny in general, together with their understandable interest in keeping disclosure of sensitive intelligence material to an absolute minimum. As the Court noted in *Klass*, however, judicial scrutiny of executive action that involves serious interference in privacy is one of the basic safeguards of the rule of law. As for the need to maintain operational secrecy, there is already an established pool of High Court judges with the necessary security clearance to hear appeals in cases involving control orders, terrorist asset-freezing orders, and deportation on grounds of national security, not to mention the Surveillance Commissioners who are tasked with authorising the use of intrusive surveillance by the police under Part 2 of RIPA. Either group would be extremely well-placed to take on the task of hearing applications for interception warrants.

90. The lack of any independent assessment of the necessity and proportionality of interception decisions is even more acute in those cases of interception which do not even require a warrant, especially in the interception in prisons where the communications in question may be subject to legal professional privilege (LPP). In January 2008, for instance, it emerged that several phone calls between Harry Roberts, a prisoner at HMP Channings Wood, and his solicitor in late 2005 and early 2006 had been secretly recorded by the Prison Service and Derbyshire Police without proper authorisation. Following an investigation, the then-Justice Secretary Jack Straw made a statement to Parliament explaining the safeguards in place to prevent unnecessary interception of privileged communications in prisons:[227]

> The PIN phone system—so called because prisoners are given a personal identification number (PIN)—intercepts and records all telephone calls that prisoners make, *except those identified by the prisoner as legally privileged or otherwise confidential communications (for example with the Samaritans)*. All intercepted telephone communications are recorded by the PIN system and initially stored on the hard drive of the system before being copied onto either a tape or CD for retention purposes. Only those prisoners who pose the greatest risk have all their communications monitored but all establishments will undertake an element of random monitoring of telephone communications of no more than 5 per cent of calls made on a particular day … *The PIN phone system is configured in such a way that it does not intercept communications between a prisoner and their legal representative or other confidential communications provided that these numbers are declared as being confidential.* This is what is termed the confidential side of the PIN system—it is not subject to interception. *However, in very limited circumstances, for example where a prison governor or law enforcement agency has reasonable cause to believe that a telephone call between a prisoner and his legal adviser is of a criminal nature or would endanger prison security or the safety of others, the governor may authorise the interception, recording and monitoring of*

225. See eg, the evidence of the then-Director of Public Prosecutions, Sir Ken Macdonald QC, to the JCHR, 12 March 2007, Q27.
226. Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning* (HL 157/HC 394, 30 July 2007), para 161.
227. Hansard, HC Debates c67WS, 15 May 2008. Emphasis added.

> *such conversations by moving the legal representative's number from the confidential side of the PIN phone system to the open side, without the prisoner's knowledge.* Such communications will then be intercepted, and a member of staff will listen to them, for such period as is deemed necessary.

The Justice Secretary went on to explain that, 'given the sensitivity and seriousness of interfering with legal professional privilege', the Prison Rules would be amended. Other than the passing reference in section 4 of RIPA, interception of prisoners' communications are governed by rules 35A and 39 of the Prison Rules.[228] Prior to the revelations of unauthorised interceptions, Rule 35A provided prison governors with a general power to authorise interceptions of prisoners' communications where he believed it is necessary and proportionate to do so for one of the grounds listed in rule 35A(4) – largely the same as those set out in Article 8(2), save that 'economic well-being' is left out and the interests of 'securing or maintaining prison security or good order and discipline in prison' are included. It was not until November 2009, however, that the power of prison governors to authorise interceptions of privileged communications was prohibited:[229]

> unless the governor has reasonable cause to believe that the communication is being made with the intention of furthering a criminal purpose and unless authorised by the chief operating office of the prison service.

91. Generally speaking, a blanket policy of intercepting the *non-confidential* communications of prisoners can be justified on a number of grounds, so long as prisoners are properly notified that their communications are liable to be monitored in this way. As the Interception Commissioner noted in his most recent report, there are often good reasons to provide for a general power to monitor prisoners' communications, for example:[230]

> Failure to monitor the communications of prisoners who pose a risk to children, the public or the good order, security and discipline of the prison could place managers and staff in an indefensible position if a serious incident was to occur which could have been prevented through the gathering of intercept intelligence.

Moreover, evidence from prison interceptions has sometimes proved valuable in the investigation of crime: for instance, the Soham murderer Ian Huntley was convicted partly on the basis of transcripts of intercepted conversations between Huntley in Woodhill Prison and his accomplice Maxine Carr in Holloway prison.[231] Given that prisoners have been convicted of crimes sufficiently serious to warrant imprisonment and given the general need to maintain order and security in a prison environment, we believe that a properly-notified, blanket policy of intercepting the non-confidential communications of prisoners without prior judicial authorisation constitutes a reasonable restriction on the right to privacy under Article 8 for the purposes of preventing crime and disorder.

---

228. The Prison Rules 1999 (SI 1999/728). Although Rule 35A purports to cover all kinds of communications, Rule 39 deals specifically with a prisoner's correspondence with his legal advisers or the courts, and provides that it may only be opened and searched in the presence of the prisoner if the governer has 'reasonable cause to believe' that it either: i) contains an 'illicit enclosure'; or ii) 'its contents endanger prison security or the safety of others or are otherwise of a criminal nature'.
229. Rule 35(2A) inserted by para 5 of Schedule 1 of the Prison and Young Offender Institution (Amendment) Rules 2009 (SI 2009/3082). This has since been amended to 'the chief executive officer of the National Offender Management Service; the director responsible for national operational services of that service; or the duty director of that service' (See Schedule 1 of the Prison and Young Offender Institution (Amendment) Rules 2011 (SI 2011/1663)).
230. Kennedy, n214 above, para 8.16.
231. See *Intercept Evidence: Lifting the ban* (JUSTICE, October 2006), para 103.

92. It is plainly unacceptable, however, that authorisation to covertly intercept the legally privileged and other confidential conversations of a prisoner should be given by a senior member of the government agency responsible for managing prisons; someone who will plainly be more sympathetic to the interests of prison management and, therefore, insufficiently objective to assess whether such a serious interference with a prisoner's privacy is necessary and proportionate. The same is true, by extension, for the privileged conversations of patients in secure facilities.[232] As Lord Bingham noted in the 2001 case of *Daly*:[233]

> Any custodial order inevitably curtails the enjoyment, by the person confined, of rights enjoyed by other citizens. He cannot move freely and choose his associates as they are entitled to do. It is indeed an important objective of such an order to curtail such rights, whether to punish him or to protect other members of the public or both. But the order does not wholly deprive the person confined of all rights enjoyed by other citizens. Some rights, perhaps in an attenuated or qualified form, survive the making of the order. And it may well be that the importance of such surviving rights is enhanced by the loss or partial loss of other rights. *Among the rights which, in part at least, survive are three important rights, closely related but free standing, each of them calling for appropriate legal protection: the right of access to a court; the right of access to legal advice; and the right to communicate confidentially with a legal adviser under the seal of legal professional privilege.*

These rights are plainly too fundamental to be abridged on the say-so of a government official. As the ECtHR held in the case of *Kopp v Switzerland*, which concerned the interception of calls to and from the applicant's law firm:[234]

> It is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, *without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence.*

Consequently, the Strasbourg Court held, the Swiss legislation breached Article 8. Similarly, in 2007 the Divisional Court of Northern Ireland unanimously held that the Prison Service's proposed use of directed surveillance of privileged communications between lawyer and client breached Article 8.[235] The Divisional Court in that case drew a sharp distinction between directed surveillance (authorised, in this case, by a senior member of the Northern Ireland Police or Prison service) under RIPA and intrusive surveillance (authorised by a Surveillance Commissioner – who is required to be 'a person who has held high judicial office').[236] As the Lord Chief Justice of Northern Ireland said:[237]

---

232. Section 4(5) of RIPA.
233. *R v Secretary of State for the Home Department ex parte Daly* [2001] UKHL 26 at para 5. Emphasis added.
234. [1999] 27 EHRR 91, para 74. Emphasis added.
235. In re *C and others* [2007] NIQB 101.
236. Section 91(2) of the Police Act 1997. See also section 63 of RIPA which provides for assistant Surveillance Commissioners to be appointed not below the level of a Crown Court or Circuit Court judge in England and Wales or Northern Ireland, or a Sheriff in Scotland.
237. In re *C and others*, para 79 per Kerr LCJ. Emphasis added. See also Campbell LJ at para 14: 'In such circumstances I do not regard the authority of a senior police officer, however detached he may be from the matter under investigation, to provide a sufficient safeguard for the purposes of Art 8'. See also Girvan LJ at para 34: 'Having regard to these considerations, if the PSNI or Prison Service applied the directed surveillance provisions of RIPA to communications between lawyer and client in the police station or prison they would infringe the Article 8 rights of the solicitor and client'.

> No reason has been proffered on behalf of the respondents to justify the discrepancy in the levels of authorisation required. It appears to me to be self evident that interference with the fundamentally important right arising under Article 8 to consult a legal adviser or a medical adviser privately will be more readily justified *where there is a demonstrable measure of independence on the part of the authorising agency.* Moreover, the confidence that a legal/medical adviser and his client/patient can have in giving advice and providing information would be commensurately increased by the knowledge that no monitoring of their consultations will take place unless this has been shown *to the satisfaction of an independent person to be strictly necessary.*

93. Although the Secretary of State appealed against other aspects of the Divisional Court's decision before the House of Lords in 2009, she did not appeal against its ruling that directed surveillance of privileged communications would breach Article 8.[238] The logic of that position is plain. If the Secretary of State accepts the Divisional Court's conclusion that directed surveillance of privileged communications would breach Article 8 because of the lack of independence of Prison Service officials, it follows that she must also accept that *interception* of privileged communications authorised by a senior Prison Service official[239] would similarly breach Article 8. We, therefore, recommend that prior judicial authorisation be required for any interception of privileged communications of persons in custody.

Inadequate ex post facto oversight

94. As noted above, the government has frequently defended the lack of prior judicial authorisation for interception warrants under Part 1 of RIPA by pointing to the supervisory role played by the Interception of Communications Commissioner (Interception Commissioner), who is required by section 57 of RIPA to be a person who 'holds or has held high judicial office'. The office of Interception Commissioner predates RIPA, having been first established in 1980 on a non-statutory basis and on a statutory basis under the Interception of Communications Act 1985.

95. The first Interception Commissioner under RIPA was Sir Swinton Thomas, a retired Court of Appeal judge, who stepped down in 2006. The present incumbent is Sir Paul Kennedy, also formerly a Court of Appeal judge, whose term will conclude in December 2012. The Commissioner produces an annual report summarising his work over the previous year. This includes: i) reviewing applications for interception warrants; ii) visiting agencies and communications providers responsible for interceptions; iii) any mistakes he has encountered in the execution of warrants; iv) his views about any relevant legal issues; and v) any other concerns he wishes to highlight about arrangements for carrying out interceptions. His oversight of communications data requests is discussed in Chapter 4.

96. In principle, the appointment of a senior judge or retired senior judge to provide oversight of Part 1 of RIPA should be an important safeguard against the unnecessary or disproportionate use of interception powers. In practice, however, the Interception Commissioner seems to us to offer a less than adequate check against the possibility of disproportionate interception, for the following reasons:

---

238. See *In re McE* [2009] UKHL 15 at paras 52-53 per Lord Phillips; para 60 per Lord Hope; para 113 per Lord Neuberger.
239. The National Offender Management Service (NOMS) was created in 2004, combining the work of the National Probation Service and the Prison Service.

a) his remit is too narrow;

b) he appears to review only a small proportion of warrants made;

c) he has no power to quash a defective warrant;

d) he has never once publicly questioned an interception decision made by the Secretary of State on human rights grounds; and

e) his work in general lacks sufficient transparency.

97. First, the Interception Commissioner's remit does not cover all lawful interceptions under Part 1 of RIPA. As noted earlier, it includes interception warrants and communication data requests but not interceptions without warrant. In 2002, however, the Commissioner agreed to provide non-statutory supervision of interceptions in prisons.[240] Even so, this still leaves a very large number of lawful interceptions that remain entirely unsupervised: in addition to secure mental health facilities and private prisons that appear to remain outside the Commissioner's remit, there is no statutory oversight for the very wide range of so-called 'private' interceptions, including interceptions of employees communications by their employers; the monitoring of calls for business purposes (deemed to be where both parties consent or – significantly – are 'reasonably believed' to consent),[241] as well as interceptions by communication service providers that:[242]

> take place for purposes connected with the provision or operation of a [telecommunications] service or with the enforcement of … any enactment relating to the use of … telecommunications services.

Although there are certainly some good reasons to treat these interceptions differently from those for law enforcement and intelligence services, it is striking that there remains no provision in RIPA for these interceptions to be subject to any kind of oversight or scrutiny.[243] More generally, the lack of any mechanism to deal with complaints of this kind of wrongful interception was highlighted by the discovery in 2008 that BT and US marketer Phorm had, two years previously, secretly intercepted the Internet sessions of 18,000 of its customers as part of an advertising software trial.[244] Similarly, the ongoing revelations of the scale of phone-hacking by the *News of the World* have brought this issue into renewed focus. In April 2009, the European Commission launched infringement action against the UK government, alleging among other things that the provisions of RIPA failed to provide sufficient protection against unlawful interception of communications, contrary to EU law,[245] and in September 2010, it referred the matter to the Court of Justice of the European Union.[246] In response to this, the Home Office quietly rushed out a consultation paper on so-called 'lawful interception'

240. See n204 above.
241. Section 3(1).
242. Section 3(3).
243. See also the 2009 report of the House of Lords Constitution Committee, n72 above, para 257: 'We recommend that the Chief Surveillance Commissioner and the Interception of Communications Commissioner should introduce more flexibility to their inspection regimes, so that they can promptly investigate cases where there is widespread concern that powers under the Regulation of Investigatory Powers Act 2000 have been used disproportionately or unnecessarily, and that they seek appropriate advice from the Information Commissioner'.
244. See n35 above.
245. See p6 below for further details of the Commission's investigations.
246. See eg, 'Commission refers UK to court over privacy and personal data protection', EU Commission press statement, 30 September 2010 (IP/10/1215).

in November 2010.[247] Among other things, it proposed removing the 'reasonable belief' provision in section 3(1) of RIPA, considerably expanding the remit of the Interception Commissioner to investigate complaints against communication service providers and, where necessary, enabling him to issue penalty notices for the 'unintentional' interception of communications. This has now been partly implemented by a statutory order made in May 2011.[248]

98. In July 2011, the report of the House of Commons Home Affairs Committee into phone hacking by the *News of the World* further highlighted the lack of oversight in this area, noting that the Interception Commissioner:[249]

> has no duties in respect of private sector operators, and in particular has no remit or resources to advise individuals who believe they have been victims of unauthorised interception of their communications by the private sector.

The Committee concluded:[250]

> The lack of a regulatory authority under the Regulation of Investigatory Powers Act has a number of serious consequences. Although the Information Commissioner's office provides some advice, there is no formal mechanism for either those who know they are in danger of breaking the law or those whose communications may be or have been intercepted to obtain information and advice. Moreover, the only avenue if anyone is suspected of unauthorised interception is to prosecute a criminal offence, which, as the Information Commissioner noted, is a high hurdle in terms of standard of proof as well as penalty. Especially given the apparent increase of hacking in areas such as child custody battles and matrimonial disputes, and the consequential danger of either the police being swamped or the law becoming unenforceable, *there is a strong argument for introducing a more flexible approach to the regime, with the intention of allowing victims easier recourse to redress.*

99. Second, even in relation to those interceptions under Part 1 that he does have oversight of, the Interception Commissioner provides at best partial oversight. For a start, he does not review each and every warrant made by the various Secretaries of State. Instead, he receives a list of all the warrants made on behalf of each agency, from which he selects a random sample to inspect in further detail during one of his twice-yearly visits. In his 2005-2006 report, Sir Swinton described his approach in the following terms:[251]

> Prior to each visit, I obtain a complete list of warrants issued or renewed or cancelled since my previous visit. *I then select, largely at random, a sample of warrants for inspection.* In the course of my visit I satisfy myself that those warrants fully meet the requirements of RIPA, that proper procedures have been followed and that the

247. Home Office, *Regulation of Investigatory Powers Act 2000: Proposed Amendments Affecting Lawful Interceptions*, November 2010. The consultation was not made public by the Home Office, with a consultation period of less than a month and initially circulated only to members of the communications sector. It was only following an outcry from NGOs that the consultation was made public and the consultation period extended by two weeks. See letter to Home Office Minister Dame Pauline Neville-Jones from 6 NGOs, dated 25 November 2010: www.openrightsgroup.org/ourwork/reports/letter-to-pauline-neville-jones-re-ripa-consultation.
248. Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011 (SI 2011/1340).
249. House of Commons Home Affairs Committee, *Unauthorised tapping into or hacking of mobile communications* (HC 907, 20 July 2011), para 36.
250. Ibid, para 39. Emphasis added. The Home Office and the Home Affairs Committee's proposal to extend the remit of the Interception Commissioner to cover this is discussed below.
251. Swinton Thomas, *Report of the Interception of Communications Commissioner for 2005-2006* (HC 315, February 2007), para 12.

> relevant safeguards and Codes of Practice have been followed. During each visit I review each of the files and the supporting documents and, when necessary, discuss the cases with the officers concerned. I can view the product of interception. It is of first importance to ensure that the facts justified the use of interception in each case and that those concerned with interception fully understand the safeguards and the Codes of Practice.

In a description matching that of his predecessor virtually word-for-word, Sir Paul Kennedy said in 2009:[252]

> Prior to each visit, I obtain a complete list of warrants issued or renewed or cancelled since my previous visit. *I then select, largely at random, a sample of warrants for inspection.* These include both warrants and attendant certificates. In the course of my visit I satisfy myself that those warrants fully meet the criteria of RIPA, that proper procedures have been followed and that the relevant safeguards and Codes of Practice have been followed. During each visit I review each of the files and the supporting documents and discuss the cases with the officers concerned. I can, if I need to, view the product of interception. It is of paramount importance to ensure that the facts justified the use of interception in each case and that those concerned with interception fully understand the safeguards and the Codes of Practice.

In his 2010 report, though, Sir Paul provided a slightly different description of his method:[253]

> *My role is essentially that of a retrospective auditor of warrants, lists of which are presented to me some weeks prior to the visit itself.* The agencies and departments provide a full list of all warrants extant, modified or cancelled since the previous visit. I then make my selection. I am satisfied that the agencies provide me with a full list of authorisations, and *they often highlight particularly challenging warrants, and those that have been associated with compliance errors, to help me to decide which warrants to review.*

100. The role of the agencies in highlighting warrants for the Commissioner is no doubt helpful and section 58 of RIPA imposes a duty on all relevant officials to 'disclose or provide' to the Commissioner 'all such documents and information as he may require' for the purpose of carrying out his functions under section 57.[254] However, it also underlines how much the Commissioner relies on agency cooperation in order to perform his task. This is particularly important given the apparently limited amount of time that the Commissioner spends on ex post facto review of interception warrants.

101. In the Interception Commissioner's latest annual report, for instance, the inspection process is described in a table which sets out the various stages involved, including the 'selection stage' in which the Commissioner:[255]

> dip-samples a number of warrants and authorisations for further scrutiny on *inspection day.*

252. Kennedy, *Report of the Interception of Communications Commissioner for 2009* (HC 341, July 2010), para 2.1.
253. Kennedy, *Report of the Interception of Communications Commissioner for 2010* (HC 1239, June 2011), para 2.7. Emphasis added.
254. Section 58(1).
255. See 'Figure 3: an inspection visit' on pg 13 of Kennedy, n253 above, Emphasis added.

The purpose of this sampling is said to be to 'ensure the random nature of inspections and ensure all warrants have an equal chance of being selected for review'. No mention is made, however, of the *proportion* of warrants that are inspected by the Commissioner. Whether the sample size is 1 in 10, 1 in 20 or even 1 in 50 is, therefore, unknown. The actual amount of time the Commissioner spends considering the warrants selected is also unknown but the reference to the 'inspection day' stage suggests that he only spends one day per agency per visit 'reading through and scrutinising warrantry paperwork'.[256] This would mean that – of the 11 agencies able to apply for interception warrants – the Commissioner spends only two days a year examining their files, or 22 days in total. His most recent report shows that 1,865 warrants were issued in 2010 by the Home Secretary and the Scottish Executive.[257] The number of warrants made by the Northern Ireland Secretary and the Foreign Secretary remains unknown.

102. But even if we were to assume for the sake of argument that the published number of warrants was spread evenly across each agency (which of course it will not be), making them each responsible for at least 170 warrants annually, then the Interception Commissioner would have at most two days per agency to read through the paperwork on every interception warrant, or 85 warrants in each daily visit. By way of comparison, nobody would expect that a judge who *granted* 85 warrants in a single day, or reviewed 85 warrants on appeal in a single day, would have time to properly scrutinise them all. We know, in any event, that this estimate cannot reflect the Interception Commissioner's actual workload because: i) the true number of interception warrants issued annually by the relevant Secretaries of State will inevitably be higher than the published figure of 1,865 warrants in 2010; and ii) by his own account, the Interception Commissioner does not inspect them all.

103. No reason has ever been given for the Interception Commissioner's decision not to publish the proportion of interception warrants he inspects annually. It is also impossible to see any valid national security reason for refusing to disclose this. Terrorists are unlikely to be emboldened by the knowledge that the Interception Commissioner only inspects 20 per cent of warrants, for example, rather than, say, 30 per cent. A collateral reason might be that the Commissioner wishes to discourage the agencies themselves from taking risks in the knowledge that he would be unlikely to discover their misfeasance, but this would be at odds with the description given by successive Commissioners of their diligence and willingness to cooperate.[258] It is difficult to avoid the impression that the real reason for not disclosing the proportion of warrants inspected by the Commissioner is because the average proportion is relatively small and this would attract adverse public criticism of his general effectiveness.

104. It is plain, of course, from his annual reports that the Commissioner's work is not confined to inspection visits of the agencies but also takes in visits to prison facilities and communication service providers, not to mention various other meetings with relevant officials. In this regard, we do not doubt that successive Commissioners under RIPA have carried out their work with considerable diligence. Nonetheless, it has never been clear whether the appointment of Interception

256. Ibid, pg 13, fig 3.
257. Ibid, pg 17, fig 4.
258. As Sir Swinton said in his 2004 report (HC 549, November 2005), para 9: 'I continue to be impressed by the quality, dedication and enthusiasm of the personnel carrying out this work on behalf of the government and the people of the United Kingdom. They should know that they have a detailed understanding of the legislation and strive assiduously to comply with the statutory criteria...'; Or as Sir Paul put it in his 2009 report: 'I continue to be impressed by the quality, dedication and enthusiasm of the personnel carrying out this work. They possess a detailed understanding of the legislation and are always anxious to ensure that they comply both with the legislation and the appropriate safeguards' (HC 341, July 2010) para 2.2. See also, Kennedy, HC 1239, June 2011, para 2.10: 'my relationship with the agencies and departments I oversee is based on equal levels of trust, mutual understanding and constructive comment'.

Commissioner is a full-time or part-time one, although the evidence available points to the latter. In December 2009, for instance, the current Commissioner, Sir Paul Kennedy, was appointed to hear MPs appeals from decisions of the expenses auditor Sir Thomas Legg.[259] If the position of Interception Commissioner is a part-time one, however, it would be good to know exactly how many days a year is spent working in this oversight capacity. Again, we can see no reason why this information should not be made public.

105. Third, the Interception Commissioner has no power to quash a defective warrant should he discover one. Nor is he able to refer a matter to the IPT should he consider that a breach of Article 8 has taken place. Under section 58(2), he has the power to report any contravention of RIPA that falls within his remit to the Prime Minister but there is no corresponding obligation on the Prime Minister to make this finding public. He may also report to the Prime Minister any concerns he may have over the adequacy of Part 1 of RIPA in respect of the interception process,[260] as well as any other matter relating to his functions that he may see fit to raise.[261]

106. Fourth, at least as far as we are able to tell from his annual reports, the Commissioner has apparently never reviewed an interception warrant in which he judged the Secretary of State's decision to be either unnecessary or disproportionate under Article 8(2). Given that more than 20,000 warrants have been made in the past decade, this suggests one of three possibilities. The first is that the relevant Secretaries of State have not, in fact, ever made an interception decision that was unnecessary or disproportionate. This would be welcome but also somewhat improbable. In the past decade, for instance, the House of Lords and the ECtHR have made a number of adverse judgments against the government for unnecessary and disproportionate interference with Convention rights, including Article 8.[262] It seems difficult to believe that the decisions of government ministers have somehow remained uniquely free of error when it comes to interception.[263]

107. The second possibility is that some interception warrants issued by the Secretary of State have indeed breached Article 8 but this has not been discovered by the Interception Commissioner. This seems more likely, particularly given that the number of warrants reviewed annually by the Commissioner during his inspection visits appears to be relatively low. The third possibility is that the Interception Commissioner has reviewed warrants involving possible breaches of Article 8 but has not highlighted them because he is slow to second-guess the decisions of the relevant Secretary of State when it comes to assessing necessity and proportionality. There is some support for this approach in case-law, particularly in relation to matters of national security. As Lord Hoffmann said in *Rehman* shortly after the 9/11 attacks:[264]

> [The attacks] are a reminder that in matters of national security, the cost of failure can be high. This seems to me to underline the need for the judicial arm of government to respect the decisions of ministers of the Crown on the question of whether support for terrorist activities in a foreign country constitutes a threat to national security. It

259. See House of Commons Members Estimate Committee, *Review of Past ACA Payments* (HC 348, 4 February 2010), Appendix 2.
260. Section 58(3).
261. Section 58(5).
262. See eg, *A and others v Secretary of State for the Home Department (No 1)* [2004] UKHL 56; S *and Marper v United Kingdom* [2008] ECHR 1581; *R (Baiai and others) v Secretary of State for the Home* Department [2008] UKHL 53; *EB (Kosovo) v Secretary of State for the Home* Department [2008] UKHL 41; *EM (Lebanon) v Secretary of State for the Home* Department [2008] UKHL 64; *R (Wright and others) v Secretary of State for Health* [2009] UKHL 3; *Gillan and Quinton v United Kingdom* (2010) 50 EHRR 45; *R (F) v Secretary of State for the Home Department* [2010] UKHL 17; *ZH (Tanzania) v Secretary of State for the Home Department* [2011] UKSC 4.
263. See also the discussion in Chapter 9 of the incredibly low success rate of complaints to the IPT.
264. *Secretary of State for the Home Department v Rehman* [2001] UKHL 47, para 62.

> is not only that the executive has access to special information and expertise in these matters. It is also that such decisions, with serious potential results for the community, require a legitimacy which can be conferred only by entrusting them to persons responsible to the community through the democratic process. If the people are to accept the consequences of such decisions, they must be made by persons whom the people have elected and whom they can remove.

However, Lord Hoffman's dicta is hardly the last word on this issue. As Lord Bingham wrote in his judgment in the Belmarsh case three years later:[265]

> It is of course true that the judges in this country are not elected and are not answerable to Parliament. It is also of course true … that Parliament, the executive and the courts have different functions. But the function of independent judges charged to interpret and apply the law is universally recognised as a cardinal feature of the modern democratic state, a cornerstone of the rule of law itself. The Attorney General is fully entitled to insist on the proper limits of judicial authority, but he is wrong to stigmatise judicial decision-making as in some way undemocratic. It is particularly inappropriate in a case such as the present in which Parliament has expressly legislated in section 6 of the 1998 Act to render unlawful any act of a public authority, including a court, incompatible with a Convention right…

The problem is that there is simply no indication from any of the Interception Commissioner's reports over the last decade as to the legal principles that he applies when reviewing the Secretary of State's decisions. We, therefore, have no way of knowing whether he is applying the right principles, let alone whether he is applying them correctly.

108. Fifth and more generally, the oversight work of the Interception Commissioner lacks sufficient transparency. This is particularly important given the generally secret nature of interception activities. The Commissioner is, after all, the only independent reassurance that the public has, not only that their communications are not being unnecessarily intercepted, but also that the law on interception is being correctly applied. His work is, therefore, essential to ensuring democratic oversight over – and accountability of – an otherwise secret interception regime.[266] In his final report as Interception Commissioner, Sir Swinton Thomas noted longstanding criticism of his lack of transparency and offered the following defence:[267]

> Over the past six years I have from time to time been subjected to criticism in the media for being oversecretive. I understand this criticism and, in many ways I would wish to be more open and transparent, but when dealing with work which is by its nature secret, that is not always possible. Balancing the requirements of secrecy with a desire for transparency is difficult to achieve. I am conscious that my Reports may appear to be bland, but I have made them as open as is possible in the circumstances, and this year the Report will be rather fuller on some issues than it has been in

265. *A and others v Secretary of State for the Home Department (No 1)* [2004] UKHL 56, para 42.
266. As the ECtHR noted in *Klass*, n138 above, powers of secret surveillance are 'tolerable ... only in so far as strictly necessary for safeguarding democratic institutions' (para 42). Independent oversight is also vital given the daunting evidential challenges faced by an applicant: 'In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue' (para 59).
267. Swinton Thomas, *Report of the Interception of Communications Commissioner for 2005-2006* (HC 315, February 2007), para 3.

> previous years. Those matters which cannot be fully explained without disclosing sensitive information relating to particular Agencies or to individuals concerned are contained in the Confidential Annex.

The need to maintain a certain degree of operational secrecy is understandable. However, it does nothing to explain why the transparency of the Interception Commissioner fares so poorly when compared to that of equivalent interception oversight bodies in other common law countries,[268] not to mention that of the Surveillance Commissioners under Part 2 of RIPA.[269] The Office of the Surveillance Commissioners has, for example, had a website for several years together with an email address welcoming feedback from the public. By contrast, there are no published contact details for the Interception of Communications Commissioner available anywhere. His annual report gives his address as the Home Office but even this has proved unreliable in the past. Letters sent by JUSTICE to Sir Swinton Thomas care of the Home Office during his tenure as Commissioner, for example, were returned bearing the statement 'not known at this address'. Letters addressed to the current Commissioner, Sir Paul Kennedy, care of the Home Office appear to reach him, but his office still has no published phone number, fax number, email address or website.

109. The Interception Commissioner's general lack of transparency is even more apparent from his annual reports which, for most members of the public, is the only evidence that he even exists. As we have already seen, these have relied heavily on rote description, with large sections of text having been either slightly rewritten or simply repeated verbatim year after year. It is difficult to see why operational secrecy should require this. The most recent report released in June 2011 is a notable exception, however, and represents a marked improvement over previous years. To their credit, the annual reports have also done a reasonable job of recording errors made by the agencies and communication service providers in applying and executing interception warrants. In almost every case, however, these have tended to be accounts of technical errors, eg, a wrong number being entered leading to the accidental interception of someone else's phonecalls by mistake, with no other information provided that would enable a reasonable person to satisfy himself or herself that the Commissioner's assessment was correct.[270]

110. Moreover, as noted above, the Commissioner appears never to have encountered an interception decision that he thought might have been disproportionate. Indeed, only once in the past decade has the Interception Commissioner recorded a case of deliberate misuse of interception powers, and the account he gives of it in his 2008 report is typical of the general lack of detail provided:[271]

> The error which was deliberate … was made by a police officer. It has no security implications, there was no invasion of privacy and because it has been reported to the relevant prosecuting authority I say no more about it in this part of my Report.

111. Probably the most valuable parts of the Interception Commissioner's reports have been his work highlighting the apparently low standards of prison interceptions. But even in this area, there have been significant shortcomings in his oversight.

---

268. See eg, *Annual report on the use of electronic surveillance 2010* (Public Safety Canada, 2011); 2010 report of the Department of Justice to Congress on the Foreign Intelligence Surveillance Act, 29 April 2011.
269. See Chapters 5 and 6 below.
270. See eg, Kennedy, *Report of the Interception of Communications Commissioner for 2008* (HC 901, July 2009), para 2.16: 'None of the breaches or errors was deliberate ... all were caused by human error or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error'.
271. Ibid, para 2.32.

112. In 2007, for instance, the Northern Ireland Divisional Court ruled that directed surveillance of privileged communications in prisons breached Article 8 because of the lack of prior judicial authorisation. The Secretary of State accepted the court's ruling and directed that all such surveillance should be authorised as 'intrusive' surveillance instead. It should have been obvious to anyone familiar with the issue, however, that this produced an obvious anomaly between the authorisation required for interception of privileged communications under Part 1 of RIPA and that required for surveillance of privileged communications under Part 2.

113. Specifically, if the prison service wanted to plant a surveillance device to listen to a prisoner's conversation with his lawyer during a face-to-face consultation, the new rules required them to seek authorisation from a Surveillance Commissioner, a judicial figure. If, however, they wanted to intercept the prisoner talking on the phone with his lawyer, they would need only the prison governor's authorisation. A member of the public might reasonably expect an issue of this significance to be addressed in the Interception Commissioner's annual report. In his 2007 report, however, the Commissioner merely noted that prisoners' communications which are subject to legal privilege 'are protected'.[272]

114. Similarly, in his 2008 report, where one might have expected some discussion of the revelation that HM Channings Wood had been unlawfully intercepting the privileged communications of a solicitor, the only reference was as follows:[273]

> Following a case which received national coverage in the media last year a review was conducted and the Prison Service has introduced new measures which are designed to prevent breaches of Articles 6 and 8 of the European Convention on Human Rights.

115. And when, in 2009, the House of Lords in *In re McE* confirmed the Divisional Court's ruling on Article 8 and the importance of prior judicial authorisation when listening in on privileged communications,[274] the Commissioner confined himself to explaining the safeguards offered by the PIN system:[275]

> Generally [the PIN system] should act as a good safeguard and prevent any legally privileged conservations being monitored unintentionally but it is not totally failsafe. Towards the end of last year the Prison Service introduced new measures which are designed to prevent breaches of Articles 6 and 8 of the Human Rights Act. In reality the system still relies heavily upon manual intervention, and so no guarantee can be given that a breach will never occur in the future. However, providing the prisoners and their lawyers always adhere to the rules and the prison staff apply the process diligently, the risk of legally privileged communications being intercepted will be minimised.

By his 2010 report, Sir Paul had reverted to his earlier, anodyne comment that 'communications which are subject to legal privilege are protected'.[276] In other words, a member of the public who relied on Sir Paul's reports over this period would have no clue that the statutory power to intercept

272. See *Report of the Interception of Communications Commissioner for 2007* (HC 947, July 2008), para 4.2.
273. 2008 report, n270 above, para 4.3
274. See eg, the comments of Lord Phillips in *In re McE*, n238 above, at para 41: 'It would not be incompatible with the Convention for power [to intercept privileged communications] to be granted in exceptional circumstances to carry out such surveillance, but I consider that the power should be granted by a statute that adequately defined those circumstances and prescribed who was to ascertain that they existed. *It seems likely that the Strasbourg Court would expect such persons to have judicial status*'. Emphasis added.
275. *Report of the Interception of Communications Commissioner for 2009* (HC 341, July 2010), para 4.3.
276. *Report of the Interception of Communications Commissioner for 2010* (HC 1239, June 2011), para 8.4.
277. Ibid, para 4.4.

privileged communications of prisoners even existed, let alone that the law as it stood risked obvious incompatibility with Article 8. This is even more striking when one considers the relatively detailed guidance in Chapter 3 of the Interception of Communications Code of Practice concerning interception of privileged communications under warrant.

116. Another instance of his lack of transparency is the Interception Commissioner's ongoing refusal to publish the total number of interception warrants issued each year. In fairness to individual office-holders, this has been a longstanding practice of successive Interception Commissioners since the early 1980s. Nonetheless, each Commissioner has had the opportunity to reverse the policy and each has declined. As Sir Paul explained in his most recent report:[277]

> I have decided to continue with the practice of previous years in not disclosing details of the numbers of [Northern Ireland and overseas] warrants in the open section of my report. This is because I remain convinced that the disclosure of Home Secretary warrants does not provide hostile agencies with any indications of targets as the total number includes both warrants issued in the interest of national security and for the prevention and detection of serious crime. In the case of Scottish Government warrants, the numbers disclosed represent the total number of serious crime warrants. *In the case of Foreign Office and Northern Ireland warrants, however, I believe it is prejudicial to national security to disclose warrantry statistics outside of the Confidential Annex as it may enable hostile agencies to estimate even approximately the extent to which any interception of communications was being undertaken to protect national security.*

This argument might seem more credible, however, were it not for the fact that, between 1980 and 1984, the annual number of interception warrants issued by the Foreign Secretary *was* made public without apparent damage to the UK's national security. Indeed, we know that the Foreign Secretary issued a total of 553 warrants between 1980 and 1984, a period which included the Soviet invasion of Afghanistan and the Falklands War. Similarly, the United States Department of Justice has for many years published annual reports to Congress which detail the number of interception warrants made under the Foreign Intelligence Surveillance Act without apparent damage to its own national security.[278] In 2010, for instance, it issued 1,579 warrants.

117. There is, moreover, an obvious contradiction between the Commissioner's reasons for publishing the number of warrants issued by the Home Secretary but not those of the Northern Ireland Secretary or Foreign Secretary. Publishing the number of warrants made by the Home Secretary 'does not provide hostile agencies with any indication of targets' as these are issued both on grounds of national security and law enforcement. But this is equally true, of course, in relation to interception warrants in Northern Ireland: no doubt a number of warrants will be on national security grounds but others will be made for law enforcement purposes (indeed there is likely to be a considerable overlap when it comes to the longstanding involvement of various NI paramilitary groups in serious organised crime). The same is also true of the Foreign Secretary, who may issue warrants not only on national security or law enforcement grounds (eg, drug trafficking) but also, notably, in the interests of 'the economic well-being of the United Kingdom'. Just as the number of warrants made by the Home Secretary offers no means of deducing how many have been made on law enforcement grounds as opposed to national security, there is no way to 'estimate even

278. See eg, www.fas.org/irp/agency/doj/fisa/2010rept.pdf or epic.org/privacy/wiretap/stats/fisa_stats.html.

approximately' from the total number of warrants what proportion the Foreign Secretary makes on national security grounds and what proportion he makes, for example, safeguarding the UK's butter exports to China. It is, therefore, difficult to take seriously the Commissioner's claim that non-disclosure should be necessary on national security grounds, particularly – as noted earlier – the number of warrants provides only a very rough indication of the actual volume of communications intercepted by each warrant.

Poor drafting and failure to keep pace with technology

118. Another key defect of Part 1 of RIPA is its poor drafting, which has led – amongst other things – to the failure of the Metropolitan police to properly investigate the extent of phone hacking by the *News of the World* between 2005 and 2011; BT's unlawful interception of 18,000 customers Internet usage in 2006; as well as a general lack of clarity. The drafting of Part 1 of RIPA also failed to anticipate the increasing overlap between different communication technologies, eg, the Internet and digital telephony, notwithstanding that these changes were already well-underway at the time that RIPA was drafted. As we shall see, RIPA's lack of clarity and failure to keep pace with new technologies has opened up a number of loopholes, thereby increasing the risk that individuals will have their interceptions wrongly intercepted in breach of Article 8(2).

119. First, the quality of the drafting of RIPA has been the subject of considerable criticism over the years.[279] In 2002, for instance, a prosecution of three police detectives for allegedly passing information to a known criminal collapsed because the trial judge ruled that section 17(1) of RIPA prevented the defendants from challenging the Crown's evidence obtained from a pre-RIPA interception of the police internal phone system. This led the Attorney General to refer the matter to the Criminal Division of the Court of Appeal for clarification. In its ruling in June 2003, the Criminal Division described RIPA as 'a particularly puzzling statute'. Noting Lord Mustill's description of the earlier Interception of Communications Act 1985 as a 'short but difficult statute', the Criminal Division added that RIPA, too, was 'a difficult statute (if somewhat longer)'.[280] So difficult were the legal issues raised by section 17 of the Act that the Criminal Division decided to refer the matter onwards to the House of Lords. In his 2004 judgment, the Senior Law Lord Lord Bingham described Part 1 of RIPA as follows:[281]

> If … the 1985 Act was a 'short but difficult statute', the 2000 Act *is both longer and even more perplexing*. The trial judge and the Court of Appeal found it difficult to construe the provisions of the Act with confidence, *and the House has experienced the same difficulty.*

His colleague Lord Steyn added his own observation that RIPA was 'not easy to understand'.[282]

279. See eg, Association of Chief Police Officers, *Review of the Regulation of Investigatory Powers Act* (2006), p42: 'The Review found the legislation had several ambiguities and deficiencies and had been implemented poorly. There was diverse interpretation and application of the law, and the training provided within the law enforcement community had been piecemeal'; Ben and Charles Raab, *Protecting Information Privacy* (Equality and Human Rights Commission, August 2011) at p37: 'Although RIPA is now the primary means by which police surveillance is regulated in the UK – and is therefore legislation that most police officers are required to be familiar with – in many places it is poorly drafted and its overall structure is far from clear'; *C v the Police and Secretary of State for the Home Department* (IPT/03/32/H,14 November 2006), para 22 per Mummery LJ: 'The experience of the tribunal over the last five years has been that RIPA is a complex and difficult piece of legislation'.
280. *R v W* [2003] EWCA Crim 1632 at para 98.
281. *Attorney General's Reference No 5 of 2002* [2004] UKHL 40 at para 9. Emphasis added.
282. Ibid, para 29.

120. If, however, the UK's most senior judges have found the provisions of Part 1 of RIPA confusing, it should come as little surprise that it has also given rise to serious difficulty for those public officials tasked with applying it. For instance, section 1(1) of RIPA makes it a criminal offence for a person to 'intentionally and without lawful authority' intercept any communication 'in the course of its transmission'. The meaning of 'interception' is further explained in section 2. In particular, section 2(7) provides that:

> For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system *shall be taken to include any time when the system … is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.*

In September 2009, however, Assistant Commissioner John Yates gave evidence to the House of Commons Committee on Culture, Media and Sport in which he stated with some confidence that the Metropolitan Police did not regard the activity of hacking into another person's voicemail as a criminal offence if the voicemail had already been listened to by its intended recipient:[283]

> ***Q1898 Chairman:*** One of the reasons given by the DPP to us is that, in order to prove a criminal offence, you have to demonstrate that the phone message was intercepted and listened to before the intended recipient had himself opened and listened to it, and that was the criminal act. That is correct?
>
> ***Mr Yates:*** Yes, the analogy is the envelope and the opened letter. It is not an offence to read the opened letter, but it is an offence to open the letter and read it, and that is the analogy.
>
> ***Q1899 Chairman:*** However, let us say that somebody is accessing my voice messages and, therefore, if they get to that voice message before I have got round to listening to it, they are committing a criminal offence?
>
> ***Mr Yates:*** Yes.
>
> ***Q1900 Chairman:*** If I happen to have listened to it and not deleted it and they then manage to access it, that is perfectly legal?
>
> ***Mr Yates:*** It is a breach of privacy. I am not sure it is legal, *but it is certainly no offence under section 1 of RIPA.*

The written evidence of the Crown Prosecution Service to the same committee initially appeared to support this analysis[284] but this was later subject to considerable clarification by the Director of

283. Evidence to the House of Commons Committee on Culture, Media and Sport, 2 September 2009, Qs 1898-1900. Emphasis added. See also the Committee's report, *Press Standards, Privacy and Libel* (HC 362, 24 February 2010), para 465: 'The police ... told us that under section 1 of the Regulation of Investigatory Powers Act (RIPA) it is only a criminal offence to access someone else's voicemail message if they have not already listened to it themselves. This means that to prove a criminal offence has taken place it has to be proved that the intended recipient had not already listened to the message. This means that the hacking of messages that have already been opened is not a criminal offence and the only action the victim can take is to pursue a breach of privacy, which we find a strange position in law'.
284. See 'Further written evidence submitted by the Crown Prosecution Service' dated July 2009: 'THE LAW: To prove the criminal offence of interception the prosecution must prove that the actual message was intercepted prior to it being accessed by the intended recipient'.

Public Prosecutions (DPP).[285] The DPP did confirm, however, that David Perry QC, the lead Treasury Counsel in criminal matters, had provisionally advised in 2005 that the proviso in section 2(7) might only extend the time of the communication under section 1(1) 'until the intended recipient has collected it'. This advice was in turn based on a very brief analysis of the proviso by the Lord Chief Justice Lord Woolf in a 2002 case involving email interception.[286] Unfortunately, as the House of Commons Home Affairs Committee noted in its report into phone hacking in July 2011:[287]

> the construction of the statute, the interpretation of the CPS's advice in 2005-2007 and the interpretation of evidence given to both us and our sister committee, the Culture Media and Sport Committee, all became the subject of dispute between Mr Yates, Mr Starmer and Mr Chris Bryant MP, with allegations of selective quotation and implications of deliberate misunderstanding of positions, and even of misleading the Committees, being made.

121. Whatever the truth of the advice given by the CPS in 2005 and 2006, however, it is disturbing that a lack of clarity over the offence of unlawfully intercepting communications should have given rise to a serious failure of investigation by the Metropolitan Police over a period of several years. In July 2011, for instance, Sue Akers, the Metropolitan Police's Deputy Assistant Commissioner in charge of the reopened investigation, told the House of Commons Home Affairs Select Committee that approximately 3,870 individuals had been identified so far, along with roughly 5,000 landline numbers and 4,000 mobile phone numbers.[288]

122. What is perhaps even more disturbing is the apparent loophole that it exposed in relation to *lawful* interceptions under Part 1 of RIPA. For if the Metropolitan Police believed in good faith that section 1(1) of RIPA did not criminalise listening to voicemail or reading email after they had been heard or read by the intended recipient, then it was surely reasonable for the police to conclude that they themselves did not need an interception warrant to intercept voicemail or email in similar circumstances. In other words, the provisional advice of senior prosecuting counsel in relation to the phone-hacking case may have been enough to drive coach and horses through the entire interception regime under Part 1. As one data protection expert told the Home Affairs Committee:[289]

> If the [Metropolitan Police's view of section 1 of RIPA] was correct, any claim that RIPA provides a high level of protection against the misuse of RIPA powers by law enforcement agencies could easily be misplaced. For instance, suppose the law enforcement agencies wanted to gain access to the content of an email Inbox: in

285. See eg, letter of the Director of Public Prosecutions Keir Starmer QC to the *Guardian,* dated 29 October 2010: *'the prosecution's approach to section 1(1) of Ripa had no bearing on the charges brought against the defendants or the legal proceedings generally. Indeed the prosecution was not even required to articulate any approach. The issue simply did not arise for determination in that case. My position is clear: a robust attitude needs to be taken to any unauthorised interception and investigations should not be inhibited by a narrow approach to the provisions in issue. The approach I have taken is therefore to advise the police and CPS prosecutors to assume that the provisions of Ripa mean that an offence may be committed if a communication is intercepted or looked into after it has been accessed by the intended recipient'.*
286. *R* (*on the application of NTL) v Ipswich Crown Court* [2002] EWHC 1585 (Admin), para 18: 'Subsection (7) has the effect of extending the time of communication until the intended recipient has collected it. It is essential on the evidence in this case that if NTL are to preserve the material, they take action before the intended recipient has collected the e-mail. Subsection (7) means that we are here concerned with what happens in the course of transmission'; the case highlights the fact that the police were still using powers under the Police and Criminal Evidence Act 1984 to request email data at a time when Part 1 of RIPA governing interceptions had already come into force, which Lord Woolf held to be lawful: 'I find it impossible to accept that it was the intention of Parliament in legislating in the terms that it did in section 1 of the RIP Act for all practical purposes to defeat the powers of the police under section 9 in this area' (para 22).
287. House of Commons Home Affairs Committee, *Unauthorised tapping into or hacking of mobile communications* (HC 907, 20 July 2011), para 30.
288. Ibid, para 89.
289. Memorandum submitted by Dr Chris Pounder of Amberhawk Training Ltd to the Home Affairs Committee inquiry.

> relation to the content of read messages, there would be no interference, and there would be no need to obtain a warrant, because RIPA is not even engaged. RIPA's warrant provisions only cover unread messages.

There is, of course, no way of knowing if any unwarranted interceptions were in fact carried out by the police in reliance on the Met's narrow reading of RIPA. Similarly, we do not know if any other agencies with interception capabilities received similar advice from their legal advisers. If any unwarranted interceptions did take place, however, it seems unlikely that they would have been detected by the Interception Commissioner for the reasons given above. More generally, the phone hacking saga shows how confidential legal advice provided in relation to secret surveillance activities may very easily undermine the ostensible safeguards of Part 1 of RIPA. It also raises the broader question of whether Part 1 can be said to meet the broader requirements of legal certainty under Article 8(2), specifically whether it is:[290]

> sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.

As the Court has repeatedly stressed, the need for 'clear, detailed rules' is particularly important when it comes to interception, 'especially as the technology available for use is continually becoming more sophisticated'.[291]

123. The same issue was also raised by the discovery in 2008 that BT and US company Phorm had secretly intercepted the Internet sessions of 18,000 of its customers as part of a trial of ad tracking software two years previously.[292] Both the Information Commissioner and the Crown Prosecution Service declined to take any action against BT or Phorm, however, and the CPS gave several reasons for its decision including that:[293]

- BT and Phorm received considerable legal advice concerning the use of this software and were advised its use was unlikely to be contrary to section 1 of RIPA. *The Home Office also provided informal advice that stated the same.* Following the second trial, BT received further and conflicting legal advice that led to it halting the covert trials. As there was no evidence to suggest either company acted in bad faith*, it could be reasonably argued that any offending was the result of an honest mistake or genuine misunderstanding of the law*;

- The trial was of limited duration and limited application. The data gathered was anonymised and processed without human intervention and later destroyed;

- There has already been an investigation by a regulator, the Information Commissioner's Office, which concluded there was 'no evidence to suggest significant detriment to the individuals involved' and took no action; and

290. *Malone*, n124 above, para 67.
291. See the cases cited at n159 above.
292. See eg, 'BT and Phorm secretly tracked 18,000 customers in 2006', by Chris Williams, the *Register,* 1 April 2008; 'BT admits tracking 18,000 users with Phorm system in 2006' by Charles Arthur, the *Guardian,* 3 April 2008.
293. See eg, 'CPS decides no prosecution of BT and Phorm for alleged interception of browsing data', CPS press statement, 8 April 2011; 'Watchdog rules out punishment over Phorm trials', ZD Net, 9 June 2008; 'Police drop investigation into BT's Phorm trials', ZD Net, 23 September 2008.

- *There is no evidence to suggest that anyone affected by the trial suffered any loss or harm as a result.*

It is, however, astonishing that both the Information Commissioner and the CPS felt able to conclude that the secret and unlawful interception of the Internet sessions of thousands of BT customers warranted neither criminal or civil sanction. It may be true that the interceptions were only meant for the purposes of market research, the data anonymised and then destroyed. But these are plainly considerations to be taken into account when determining weight of the appropriate sanction, not when determining whether the law itself has been broken. Especially surprising is the dismissive attitude taken by the CPS to what was obviously a serious and large-scale breach of privacy, on the basis that there was 'no evidence to suggest' that anyone 'suffered any loss or harm' as a result. It would surely come as little comfort to learn, for example, that the reason your postman was secretly opening your mail was because he was simply conducting his own research on which products you might be interested in, or that he was so busy opening the letters of other people as well that he didn't have time to read any of them.

124. Most surprising, however, was the disclosure that the Home Office had 'informally advised' BT and Phorm that secret interception of its customers' intercept sessions would be lawful under Part 1 of RIPA. Not only was the law sufficiently unclear that the UK's largest communications service provider thought that its actions would be legal, but so too did the government department responsible for administering RIPA. In other words, not only did the postman consider that secretly opening your mail for market research purposes might be lawful, but apparently so did the Home Office. Again the question arises: if the Home Office thought that this kind of unwarranted interception might be lawful under Part 1 of RIPA, what other questionable interception methods did they also believe might be legitimate?

125. Fortunately, the European Commission took more seriously the complaints of Internet users, and commenced infringement action against the UK government. In September 2010, it referred the government to the Court of Justice of the European Union for 'not fully implementing EU rules on the confidentiality of electronic communications such as e-mail or Internet browsing', including the ePrivacy and Data Protection Directives.[294] Specifically, the Commission complained that:

- there is no independent national authority to supervise the interception of some communications, although the establishment of such authority is required under the ePrivacy and Data Protection Directives, in particular to hear complaints regarding interception of communications;

- current UK law authorises interception of communications not only where the persons concerned have consented to interception but also when the person intercepting the communications has 'reasonable grounds for believing' that consent to do so has been given. These UK provisions do not comply with EU rules defining consent as 'freely given, specific and informed indication of a person's wishes'; and

- current UK law prohibiting and providing sanctions in cases of unlawful interception are limited to 'intentional' interception only, whereas EU law requires Members States to

294. See eg, 'Commission refers UK to court over privacy and personal data protection', EU Commission press statement, 30 September 2010 (IP/10/1215).

> prohibit and to ensure sanctions against any unlawful interception regardless of whether committed intentionally or not.

In response to this, the Home Office issued a hastily-prepared private consultation paper to industry members in November 2010 which proposed amending RIPA to cover so-called 'unintentional' interception by communication service providers and others, as well as extending the oversight remit of the Interception Commissioner.[295]

126. Developments in communications technology over the last decade have led some to defend RIPA on the grounds that the pace of change could not be easily anticipated by legislators. As the Information Commissioner told a parliamentary committee in April:[296]

> *RIPA was drafted for the wiretap age.* We are now talking about the Internet, we are now talking about deep packet inspection, we are now talking about online behavioural advertising…

The failings of RIPA, however, should not be so easily excused. First, in relation to the failure of the Metropolitan Police to properly investigate the extent of phone-hacking by the *News of the World* between 2005 and 2011, it is clear that the problems arose not from a failure of Parliament to anticipate things like voicemail, but that provisions such as section 2(7) were so poorly drafted that they failed to make clear what Parliament must surely have intended, ie, to protect voicemail and email that had already been accessed by the recipient from being unlawfully intercepted.

127. Second, although the Home Secretary claimed at its Second Reading in March 2000 that RIPA was 'designed to ensure that the intercept regime takes proper account of technological developments',[297] it is clear that its drafters not only failed to anticipate future developments in communications technology but also managed to ignore a great many changes that had already taken place by the time the Bill was introduced.

128. By early 2000, for instance, all of the UK's mobile phone providers had been operating digital networks for several years and mobile data services had also been introduced; there were approximately 11 million people in the UK who accessed the Internet on a daily basis;[298] Voice over Internet Protocol software had been commercially available since 1998; deep packet inspection was already widely used in firewalls; and the use of peer-to-peer networks had already been popularised by the launch of Napster the previous year. Indeed, as early as December 1998, the Director General of Oftel had predicted that 'in due course the telecoms companies are going to be providing voice telephony over the Internet'.[299] Even the government's own consultation paper on encryption services in 1999 noted that 'the convergence of telephony and computer technologies will make it easier for encrypted speech and data to be sent over a range of networks'.[300] If, therefore, RIPA was indeed passed for the 'wiretap age', it should have been obvious to its drafters in the Home Office that this was already a bygone era.

---

295. Home Office, *Regulation of Investigatory Powers Act 2000: Proposed amendments affecting lawful interception* (9 November 2010).
296. Evidence to the House of Commons Home Affairs Committee, 26 April 2011, Q145. Emphasis added.
297. Hansard, HC debates col 772, 6 March 2000.
298. Office of National Statistics, *Frequency of access to the Internet 2000-2003*, showing 20% of the UK population accessing the Internet 'at least once a day'.
299. 'Oftel's main man', 4 December 1998, www.computing.co.uk/ctg/feature/1835646/oftels-main.
300. Department of Trade and Industry, *Building Confidence in Electronic Commerce* (March 1999), para 58.

Intercept as evidence

129. Section 17(1)(a) of RIPA prohibits the use of material obtained by way of an intercept warrant as evidence in either criminal or civil proceedings. Section 17(1)(b) similarly prohibits any evidence that would even 'tend to suggest' that an interception warrant has been applied for, or issued, or is about to be issued. The ban on intercept does not extend, however, to interceptions without a warrant. So, for example, intercept material is admissible in court where it has been obtained:

a) with the consent of one party;

b) using a covert surveillance device, rather than a direct intercept of a communications network or service;

c) via an interception in prison or a secure mental health facility; or

d) outside the UK.

130. The UK's ban on the use of intercept as evidence reflects a long-standing government practice but has proved increasingly controversial over time, particularly among those who maintain that it is frequently the best evidence of a defendant's guilt. In our 1998 report, for instance, we noted that there was a 'growing consensus' that the ban on intercept evidence was 'now unsatisfactory' and recommended the ban should be lifted in order to bring UK law into line with the position in those of most other western countries.[301] As Lord Lloyd of Berwick, a Law Lord and former reviewer of terrorism legislation, said in 2000:[302]

> We have here a valuable source of evidence to convict criminals. It is especially valuable for convicting terrorist offenders because in cases involving terrorist crime it is very difficult to get any other evidence which can be adduced in court, for reasons with which we are all familiar. We know who the terrorists are, but we exclude the only evidence which has any chance of getting them convicted; and we are the only country in the world to do so.

131. The primary justification for the statutory ban on intercept evidence has always been the claim that their sensitive interception methods would otherwise be disclosed in open court, leading to interception capabilities being degraded. This, of course, ignores the fact that most other countries regularly use intercept evidence in open court without such loss of intercept capability, including other common law jurisdictions with similar criminal procedures and disclosure obligations to our own.

132. As we will see in subsequent chapters, however, the admissibility of material gained from surveillance is also one of the primary means by which the courts are able to ensure that the authorities comply with the law.[303] The police's failure to get the necessary authorisation for intrusive surveillance, for instance, may result in the court excluding any evidence obtained as a result.[304] As the ECtHR said only last year in *Uzun v Germany*, the possibility that evidence from illegal surveillance might be excluded by a court at trial constitutes 'an important safeguard' against arbitrary interference

301. *Under Surveillance: Covert policing and human rights standards,* p76 and recommendation 15.
302. Hansard, HL Debates col 109-110, 19 June 2000.
303. See especially Chapters 5 and 6 below.
304. See eg, *R v Fulton* [2009] NICA 39 (19 June 2009), para 13 per Girvan LJ.

with Article 8, 'as it discourage[s] the investigating authorities from collecting evidence by unlawful means'.[305] The ban on the use of intercept evidence, therefore, also prevents one of the most important kinds of judicial oversight over this area of the law.

133. Following the 9/11 attacks, the pressure to allow the use of intercept material as evidence became even more acute as a number of exceptional counter-terrorism measures – including indefinite detention without charge, control orders and the extended use of pre-charge detention – were introduced by the government on the basis that they were necessary due to the evidential difficulties involved in prosecuting suspected terrorists.[306] This was particularly problematic given that, as Lord Bingham noted in 2004, there was no human rights objection to the use of intercept evidence:[307]

> the United Kingdom practice has been to exclude the product of warranted interception from the public domain and thus to preclude its use as evidence. *But this has been a policy choice, not a requirement compelled by the Convention, and other countries have made a different policy choice.* Article 8(2) of the European Convention permits necessary and proportionate interference with the right guaranteed in Article 8(1) if in accordance with the law and if in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. *Save where necessary to preserve the security of warranted interception, there is no reason why it should have been sought to exclude the product of any lawful interception where relevant as evidence in any case whether civil or criminal.*

134. In October 2006, we published *Intercept Evidence: Lifting the ban*, in which we argued that the statutory bar on the use of intercept as evidence was 'archaic, unnecessary and counter-productive'.[308] Among other things, we noted that the UK was the only common law jurisdiction to prohibit completely the use of intercept in criminal proceedings.

135. In January 2008, the Privy Council Report on the use of Intercept as Evidence recommended that the ban be lifted, although subject to a series of 'operational requirements' that had to be met before legislation could be introduced. These included such restrictions as:[309]

- No intelligence or law enforcement agency shall be required to retain raw intercepted material for significantly more or less time than needed for operational purposes (which may include using the material as evidence); and

- No intelligence or law enforcement agency shall be required to examine, transcribe or make notes of intercepted material to a higher standard than it believes is required to meet its objectives (which may include, but are not limited to, using the material as evidence).

These 'essential security requirements' appear to have been aimed primarily at reassuring the intelligence services that lifting the ban on intercept evidence would not degrade their interception

305. *Uzun v Germany,* n174 above, para 72.
306. 'Intercept Evidence: Lifting the ban', *JUSTICE*, October 2006, pp13-17.
307. *Attorney General's Reference No 5 of 2002* [2004] UKHL 40, para 14. Emphasis added.
308. See n306 above.
309. *Report of the Privy Council Review of Intercept as Evidence* (Cm 7324, 30 January 2008), p49.

capabilities.[310] In particular, the Privy Council report recommended that the government provide an undertaking that it would 'take action' if either 'the practical operation of the regime or subsequent adverse legal rulings meant that the operational requirements set out above could no longer be met'.[311]

136. Following the Privy Council report, a Home Office working group was established to take forward the work of developing a new legal model known as 'PII Plus' to allow the use of intercept as evidence. In December 2009, however, the Home Office reported that: [312]

> despite best efforts to design, build and test the model, it does not provide a viable basis for implementation, without breaching the operation requirements set out by the Privy Council review … the 'PII Plus model' … would weaken and not enhance our ability to protect the public and to identify and bring the guilty to justice.

Specifically, the 2009 report explained, the operational requirements identified by the Privy Council meant that the PII Plus model did not 'require the retention of all intercepted material', nor did it provide for judicial control of the intercepting agencies' 'retention, examination and review processes'.[313] In particular, the Home Office noted, the 2009 judgment of the ECtHR in *Natunen v Finland* made it likely that 'full retention (or judicial control over what may be discarded) is likely to be essential to ensure fair trials under an intercept as evidence regime'.[314] Specifically, the Court in *Natunen* had held that a Finnish law that required 'superfluous' intercept material to be destroyed without judicial supervision breached the right to a fair trial under Article 6:[315]

> a procedure whereby the investigating authority itself, even when co-operating with the prosecution, attempts to assess what may or may not be relevant to the case, cannot comply with the requirements of Article 6(1) … In this case, the destruction of certain material obtained through telephone surveillance made it impossible for the defence to verify its assumptions as to its relevance *and to prove their correctness before the trial courts.*

In January 2011, the Home Secretary told Parliament that work would shortly commence on 'assessing the likely balance of advantage, cost and risk of a legally viable model for use of intercept', with 'a report back to Parliament during the summer'.[316] As of September 2011, though, no report has yet been made.

137. In our view, Lord Bingham's conclusion in 2004 that there is nothing in the European Convention on Human Rights that would prevent the use of intercept as evidence in UK courts remains correct. In particular, there is nothing in the judgment of the ECtHR in *Natunen* that would prevent the development of a perfectly workable model for the use of intercept evidence in UK courts. It is true that this would likely increase retention and transcription burdens on the intelligence services. But retention is no longer a significant issue in an age of digital storage and improved transcription is ultimately a matter of increasing resources. Nor should it come as much of a surprise that a workable

310. This has been the primary reason for maintaining the ban on intercept: see our 2006 report, pp22-28.
311. N309 above, p50.
312. *Intercept as Evidence: A Report* (December 2009, Cm 7760), paras 23-24.
313. Ibid, para 11.
314. Application no 21022/04, 31 March 2009.
315. Ibid, para 47.
316. 26 Jan 2011: col 9WS.

and compatible model of intercept evidence should conflict with the 'operational requirements' identified by the Chilcott Committee, for these were always weighted too heavily in favour of intelligence interests ahead of those of police and prosecutors. In our view, the requirements of Chilcott's Committee are mostly unnecessary and should not be allowed to stand in the way of broader reform.

138. Moreover, as our 2006 report made clear, the experience of other countries shows that the fears of the intelligence services about the operational impact of using intercept evidence are misplaced. Despite this, some commentators have continued to attack the use of international comparisons on the basis that the adversarial nature of our legal system, together with the requirements of Article 6 ECHR, mean that disclosure obligations on the prosecution 'are far more demanding and revealing than in the jurisdiction of any comparable country'.[317] This is plainly incorrect, however. Intercept evidence has been admissible for many years in such common law countries as Australia, Canada, New Zealand, South Africa and the United States. Not only do all those countries share the same adversarial legal system as our own but they also have similar disclosure requirements to those required by Article 6 ECHR. Indeed, as the recent Canadian Commission of Inquiry into the Air India bombing noted, the disclosure obligations under UK law are, in fact, less onerous than those under the Canadian Charter of Rights and Freedoms:[318]

> In general, disclosure obligations in both the United States and the United Kingdom are less broad than in Canada. Both the United States and the United Kingdom attempt to flesh-out disclosure requirements in statutes and other rules while, as discussed above, Canada relies on a case-by-case adjudication under the Charter. Both the decreased breadth and increased certainty of disclosure requirements in the United States and the United Kingdom may make it less necessary for prosecutors to claim national security confidentiality over material that may be relevant to a case, but which does not significantly weaken the prosecution's case or strengthen the accused's case.

139. Indeed, in our view, the arguments in favour of lifting the ban on intercept remain as strong as ever. In September 2009, for instance, three men were convicted of terrorism offences in relation to a conspiracy to blow up transatlantic airliners.[319] Evidence at trial included transcripts of the emails[320] sent by the plotters between the UK and Pakistan, which had been obtained via a mutual legal assistance request from Yahoo's servers in California after having been intercepted by the US National Security Agency.[321] There can be little doubt that the emails were also intercepted by the UK authorities, most likely by GCHQ, but these intercepts would have been inadmissible due to section 17 of RIPA. The fact that the Crown Prosecution Service was obliged to rely on overseas intercepts of emails sent to and from the UK in order to convict terrorists involved in a UK plot only highlights the continuing absurdity of the statutory ban.

---

317. See eg, Lord Carlile QC, *6th report of the Independent Reviewer pursuant to section 14(3) of the Prevention of Terrorism Act 2005* (3 February 2011), para 60: 'Outside commentators have made comparisons with other jurisdictions where intercept is admissible. These comparisons are ill-informed and misleading. In our adversarial legal system the requirements of disclosure of material by the prosecution to the defence (there being no equivalent requirement on the defence) are far more demanding and revealing than in the jurisdiction of any comparable country'.
318. 'Disclosure and Secrecy in other Jurisdictions'' in 'The Unique Challenges of Terrorism Prosecutions' (Ch 7, Vol 4 at p 267), *Air India Flight 182: A Canadian Tragedy* (June 2010).
319. See BBC News, 'Three guilty of airline bomb plot', 7 September 2009.
320. See BBC News, 'Airlines bomb plot: the emails', 7 September 2009: http://news.bbc.co.uk/1/hi/uk/8193501.stm.
321. 'NSA-Intercepted Emails Helped Convict Would-Be Bombers', *Wired*, 8 September 2009.

Recommendations

140. In Chapter 10, we summarise our arguments in favour of root-and-branch reform of RIPA. In this section, we summarise the key recommendations that any new law should adopt in relation to covert interception of communications.

Introduce prior judicial authorisation for interception warrants

141. The current procedure for intercepting agencies applying for an interception warrant should be retained, but the application should be made ex parte to a security-cleared High Court judge[322] rather than the Secretary of State. In sufficiently complex cases, a judge may direct the appointment of a special advocate to represent the interests of any affected person and the public interest in general.[323] In cases of emergency, there should be provision for self-authorisation by the head of the intercepting agency, to be followed by judicial confirmation within 48 hours.

142. Judicial control over interceptions would not only ensure that any interference with the private communications of affected individuals was necessary and proportionate under Article 8(2) but it would also reduce considerably the need for ex post facto oversight by the Interception of Communications Commissioner.

143. Any interception of communications by businesses and communication services providers other than by interception warrant may only take place with the consent of the person in question. In the case of interceptions in prisons and secure mental health facilities, a blanket policy of intercepting the non-confidential communications of prisoners and patients may be justified where it has been properly notified. However, any interception of the confidential and privileged communications of prisoners and patients may only be authorised under warrant from a judge.

Improve independent oversight

144. Although the transparency of his annual reports has recently improved, the oversight provided by the Interception Commissioner still falls far short of what is necessary, not only in terms of effective judicial oversight but also proper democratic scrutiny. In the first instance, this would be best remedied by the requirement that all interception warrants be issued by a judge rather than the Secretary of State. This would ensure that no warrant would be made without its legality, necessity and proportionality being assessed by an independent judicial authority.

145. More generally, as we outline further in Chapter 7, we propose any remaining oversight work of the Interception of Communications Commissioner should be folded into that of the Surveillance Commissioners, including the current non-statutory oversight of prison interceptions and those in secure mental health facilities. It is otherwise unhelpful and potentially confusing for oversight of surveillance powers to be fragmented unnecessarily. The Surveillance Commissioners would also assume the work of authorising interception warrants on the basis that they already have

322. This could either be the existing pool of High Court judges with the necessary clearance to hear cases involving closed proceedings on national security grounds or, as we propose in Chapter 7, extending the role of the Surveillance Commissioners.
323. See our 2009 report, *Secret Evidence* for further details.

considerable experience of the human rights/proportionality issues surrounding the use of intrusive surveillance.

146. The issues raised by so-called 'unintentional' interceptions by businesses and communication service providers seem to us to have more in common with those of data protection than the kind of targeted surveillance employed for law enforcement and intelligence purposes. Although the government has now narrowed the meaning of 'consent' under section 3(1) (albeit by way of secondary legislation), and given the Interception Commissioner power to issue penalty notices for 'unintentional' interception,[324] this still leaves oversight in the hands of an official with little capacity for public outreach of any kind. We, therefore, propose the Information Commissioner should take on responsibility for oversight of this area.[325] We also recommend that the available sanctions for the so-called 'unintentional' interception of communications by private bodies include both criminal and civil penalties, in order to reflect the potential seriousness of invasions of privacy caused by interceptions by private companies. In addition, unlawful *targeted* surveillance by private companies and individuals would continue to be dealt with as a criminal matter, which the Metropolitan Police now appears to be taking more seriously than it did in 2005 and 2006.

Improve clarity and flexibility of the law

147. Any new law on interception must not only reflect rapid changes in communications technology over the last two decades but also anticipate the inevitability of continuing change. In addition, although interception is undoubtedly a technical area of the law, there is no doubt that the relevant law could be drafted in much clearer terms. This in turn would provide members of the public with a much better indication than is currently provided by Part 1 of RIPA of the various circumstances in which authorities may lawfully and covertly intercept their communications for law enforcement and intelligence purposes.

Lift the ban on intercept as evidence

148. The case for lifting the statutory ban on the use of intercept evidence in criminal and civil proceedings seems to us to be inarguable. It is also best achieved in the context of broader reform of the law of interception. In particular, giving judges the responsibility of issuing interception warrants would also enable the necessary judicial control over the retention of intercept material, which was a key requirement identified by the ECtHR in *Natunen v Finland*. The operational requirements identified by the Chilcott Committee are unnecessary and should not be allowed to stand in the way of broader reform on this issue.

---

324. See n248 above.
325. See eg, the recommendation of the House of Lords Constitution Committee, n72 above, para 137: 'The Government should consider expanding the remit of the Information Commissioner to include responsibility for monitoring the effects of government and private surveillance practices on the rights of the public at large under Art 8 of the European Convention on Human Rights'.

Chapter 4
Communications Data

149. Despite its near-ubiquity, the use of communications data for surveillance is not very well-understood by the general public.[326] In particular, media reports frequently confuse the number of requests made by public authorities for access to communications data with the number of interception warrants.[327] The distinction, however, is a very simple one. Interceptions are concerned with what was said, ie, the *contents* of a message. Communications data, by contrast, is information about the who, when and where. Despite the modern terminology, therefore, the use of communications data for surveillance purposes is a very old one, eg, secretly recording the address on a letter meant for someone else. Indeed, communications data is sometimes referred to as 'envelope' data for this reason.

150. As communications technology has advanced, however, so too has the amount of data available about each individual communication. As part of his case before the Strasbourg Court in 1984, for instance, Mr Malone complained that the Post Office had secretly attached a 'meter check printer' to his phone line which had recorded 'the numbers dialled on a particular telephone and the time and duration of each call',[328] and that this information was then passed to the police. The Court noted that the Post Office's use of phone meters in general was legitimate for the purposes of providing a telecommunications service,[329] and was, therefore, distinguishable from the covert interception of his phone calls by police. But the Court also held that just because it was legitimate for the Post Office to record information about Mr Malone's phone use for its own purposes, this did not exempt the information from the protection of Article 8. In particular, the Court held, the lack of any legislative safeguards to prevent the information being passed to the police unnecessarily or disproportionately breached Article 8(2).[330]

151. The information recorded by a phone meter in the early 1980s is nothing, however, when compared to what is today recorded digitally in respect of every mobile phone call, text message or Internet session. 'Traffic data' for a phone call, for instance, includes not only the numbers of the caller and the called, the time, data and duration of the call, but also data showing the location of each party, whether the nearest telephone exchange or – increasingly – GPS data. Similarly, the traffic

326. See eg, the 2007 report of the Home Affairs Committee, n71 above, para 331: 'the provisions of RIPA in respect of communications data are not well understood'.
327. See eg, the *Daily Telegraph,* 'Phones tapped at the rate of 1000 a day', 29 January 2008.
328. *Malone*, n124 above, para 56.
329. See eg, *Malone*, ibid, para 84: 'a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service'.
330. Ibid, paras 83-88.

data associated with a single email message will typically include not only the data and time of the message, when it was sent and received, etc., but also the sender's login name and IP address, from which can be gained a variety of information including, in certain cases, the particular computer used and its location. Traffic data from an Internet session will include similar information as well as, for instance, the URLs of websites visited (eg, www.justice.org.uk), and the time spent on each site. In addition to so-called 'traffic data', communications data also includes 'service use' data produced by service providers, eg, itemised phone bills or Internet records, and 'subscriber data'; ie, the name and date of birth of the customer, their billing address, contact and payment details. Under both UK and EU law, moreover, communications service providers are required to retain relevant communications data for up to two years.[331]

152. In this sense, the idea of communications data as being purely 'envelope data' is highly misleading: nobody writes their friend's credit card details on an envelope, still less their own. It should also be obvious that the unnecessary or disproportionate disclosure of details about a person's private communications can, in some cases, be every bit as damaging to that person's privacy as an actual interception of their communications, particularly when it reveals their location at a particular time and date or the fact of their contact with a specific person.

153. Although *Malone* led to changes in the regulation of phone metering, there remained no overarching legal framework governing the access of public bodies to communications data for surveillance purposes until the enactment of RIPA in 2000.[332] Prior to that, public bodies sought data under various specific provisions, eg, section 9 of the Charities Act 1993 which grants the Charity Commission the power to request 'any information' in someone's possession which relates to any charity.[333] Chapter 2 of Part 1 of RIPA which governs requests for communications data was not brought into force until January 2004, however, largely because of ongoing controversy over the number of public bodies that would have power to make requests.[334] However, RIPA did not repeal any of the corresponding powers that public bodies had under other statutes to obtain communications data. Indeed, as Lord Macdonald QC noted in January 2011, despite the enactment of RIPA, there remains 'a wealth of other statutes' under which public bodies may gain access to communications data.[335]

154. 'Communications data' is defined by section 21. It includes traffic data, service user data and subscriber data as outlined above, but notably excludes 'the contents of a communication'.[336] In particular 'traffic data' includes any data that identifies:

a) the location where a communication is taking place (eg, its origin and destination);

b) the people involved (eg, caller and receiver, sender and addressee); or

331. See eg, Directive 2006/24/EC (5 March 2006). See also eg, Part 11 of the Anti-Terrorism Crime and Security Act 2001.
332. See eg, the report of the Privy Council Review Committee of the Anti-Terrorism Crime and Security Act 2001 (HC 100, 18 December 2003), para 382, which described the framework governing the availability of communications data to public authorities as 'diffuse'. The police and HM Customs & Excise had powers to obtain data under PACE 1984, and a broad range of other statutes made provision in specific cases. Underlying this was section 29(3) of the Data Protection Act 1998, which provided an exemption for the disclosure of personal data for the purposes of preventing or detecting crime, etc.
333. The same power is now provided by section 54 of the Charities Act 2006.
334. See para 1 of the Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003/3172).
335. Lord Macdonald of River Glaven QC, *Review of Counter-Terrorism and Security Powers* (Cm 8003, January 2011), p6.
336. Section 21(4)(b).

c) any equipment used to transmit, receive or route the communication (eg, the phone being used).

155. Requests for communications data are governed by section 22 of RIPA. It provides that each public body able to request data under RIPA has a designated person – typically a senior member of the organisation – who may request communication service providers to provide data where he believes it necessary:[337]

a) in the interests of national security;

b) for the purpose of preventing or detecting crime or of preventing disorder;

c) in the interests of the economic well being of the United Kingdom;

d) in the interests of public safety;

e) for the purpose of protecting public health;

f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;

h) for any purpose … which is specified … by the Secretary of State;

i) to assist investigations into alleged miscarriages of justice; or

j) to identify and notify the next of kin of a deceased or incapable person.

In addition, the designated person may not request the provision of communications data unless he believes that it is proportionate to do so.[338] The request to a service provider may be in the form of an authorisation (section 22(3)) or a notice (section 22(4)), the difference being the former is a request for information that the provider already holds, while a notice is a direction to the provider to acquire it on behalf of the requesting body. Notices and authorisations last one month unless renewed.[339] Service providers must comply with notices requiring access to communications data under RIPA, unless it is 'not reasonably practicable' to do so.[340] If necessary, the Secretary of State can seek an injunction for the enforcement of the notice.[341]

156. The number of public bodies able to make requests for communications data under RIPA has fluctuated considerably over time but currently includes the police, law enforcement and intelligence services; a number of government departments including the Home Office, Ministry

337. Section 22(2), as supplemented by Art 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010.
338. Section 22(5).
339. Section 23(4) and (7).
340. Section 22(7).
341. Section 22(8).

of Justice, and Ministry of Transport; various emergency services (eg, fire and rescue boards, ambulance services, etc.); all local authorities and NHS trusts; and an eclectic range of more than 100 other public bodies including the Charity Commission, the Food Standards Agency and the Pensions Regulator.[342]

157. However, not all public bodies are equal for the purposes of making communication data requests. First, for a number of public bodies, the possible grounds for the making of requests listed in section 22(2) requests is limited by regulation. So, for example, the power of officials in the Criminal Cases Review Commission to make requests is restricted solely to investigating miscarriages of justice, while the power of the Scottish Ambulance Board to make requests is similarly restricted to preventing or mitigating injury or death during an emergency.[343] Second, many public authorities are restricted in the *type* of communications data they can request. For instance, the Child Maintenance and Enforcement Commission can request service user data and subscriber data but not traffic data.

158. Oversight of requests for communications data is provided by the Interception of Communications Commissioner.[344] Since late 2005, public bodies able to make requests have been subject to an inspection regime carried out by an inspectorate under the direction of a Chief Inspector and the supervision of the Commissioner.

159. Although Chapter 2 of Part 1 came into force in January 2004, statistics on the number of requests for communications data annually were not published for several years. In his annual report for 2004, the Interception Commissioner Sir Swinton Thomas had promised to provide details of the number of requests made in his 2005 report.[345] However, no report was published the following year, and it was not until February 2007 that the figures became available. Since January 2005, public bodies have made more than 2.7 million requests under RIPA.[346] The number of communication data requests made in 2004 remains unpublished to this day.

160. Although the extension of requesting powers to local authorities has attracted perhaps the most criticism, they make up only a small proportion of requests: less than 7,000 in the last six years.[347] In addition, the overwhelming proportion of local authority requests concern subscriber data rather than service use data (they have no power to request traffic data).[348] The Home Office Review of Counter-Terrorism Powers published in January 2011 similarly noted that:[349]

> The vast majority of requests by public authorities for communications data – 80% of them – are simple subscriber checks. These involve asking a CSP for the identity of the subscriber of a particular phone number, or the account-holder of a given email address. These are most frequently needed when individuals provide their numbers,

342. See schedules 1 and 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480).
343. Ibid.
344. Section 57(2)(b)). See further Chapter 3 above.
345. 2004 report (HC 549, November 2005), para 23: 'although no formal oversight regime was in place during 2004 work was, and continues to be, undertaken to gather statistical information from all the empowered police and public authorities on their use of the powers conferred on them under RIPA Part 1, Chapter 1, specifically (i) the number of requests made for subscriber details, (ii) the number of requests made for details of incoming and outgoing data, (iii) details of any other types of data, and (iv) the total number of errors that occurred during the application process. I intend on providing these details, and a report of the oversight inspections during 2005, in my 2005 Annual Report'.
346. Source: annual reports of the Interception of Communications Commissioner.
347. Ibid.
348. 95% of local authority requests are for subscriber data rather than service use data: see Kennedy, 2010 report (HC 1239, June 2011), pg 41, chart 6.
349. (Cm 8004, January 2011), p28.

but give no name or a false name. This sort of check is relatively unintrusive but often provides the key information to start an investigation.

161. Unlike material obtained from interceptions under Part 1, communications data is admissible in criminal and civil proceedings, and is regularly adduced as evidence in the prosecution of a very wide range of criminal offences.

Inadequate authorisation and oversight

162. As the ECtHR made clear in its judgment in *Malone*, Article 8 requires that requests by public bodies for access to communications data must be governed by legislation in the same manner as other kinds of surveillance, including 'adequate and effective safeguards against abuse'.[350] In the case of interceptions of communication, these safeguards include authorisation by a judge or other independent body.[351] In the case of GPS surveillance, by comparison, the ECtHR has said that 'subsequent judicial review of a person's surveillance' would offer 'sufficient protection against arbitrariness'.[352] In the case of requests for a person's phone records, subscriber data or location data, however, it is clear that neither the procedures for making requests under RIPA, nor their subsequent review by the Interception Commissioner, provide the necessary safeguards against abuse by public bodies.

163. First, Chapter 2 of Part 1 of RIPA puts the power to authorise requests in the hands of a senior member of the same agency that is seeking the communications data. The precise level of authorisation required in each case is specified by regulation. If, for example, an officer from Nottinghamshire Police wanted to obtain traffic data relating to a person's Twitter account as part of an investigation into public order offences, she would need authorisation from a Superintendent in the same force.[353] And if a junior official in the Trading Standards Service (part of the Department of Enterprise, Trade and Investment) wanted to obtain a person's subscriber data as part of an investigation into a complaint about counterfeit designer goods, they would require authorisation from the Deputy Chief Inspector in the same Service.[354]

164. While it is no doubt true that senior members of organisations are typically well-placed to supervise the operational decisions of their subordinates, and more mindful of their ultimate accountability to the public, it is also clear that senior and junior members of the same organisation will inevitably share an interest in achieving the necessary results. The relative seniority of a Police Superintendent would not normally be enough, for instance, to make her sufficiently objective to authorise a search warrant, unless it was a genuine emergency and there was not sufficient time to approach a judge. Still less is it realistic to expect a Deputy Chief Inspector to be sufficiently independent of an investigation being carried out by his subordinates in the Trading Standards Service to objectively assess whether secretly accessing someone's communications data is a necessary and proportionate interference with their right to privacy.[355]

350. See eg, *Klass,* n138 above, para 50.
351. See generally Chapter 2 and also *Dumitru Popescu v Romania (no. 2)* (App no. 71525/01, 26 April 2007, paras 70-71 and *Iordachi and Others v Moldova* (App no. 25198/02, 10 February 2009), para 40.
352. *Uzun v Germany,* n174 above*,* para 72.
353. Schedule 1 of the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 480/2010).
354. Ibid, Part 2 of Schedule 2.
355. See eg, LSE Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (June 2009), p30: 'now seems a good time to question whether a senior official in an organisation with an interest in the outcome of an investigation is the best person to judge the application for access to communications data made by a junior figure in the same organisation'.

165. As the ECtHR held in *Uzun*, in the case of less intrusive types of surveillance, lack of sufficient independence at the initial authorising stage can be offset to a certain extent by subsequent judicial review. In the case of communications data, however, there is no guarantee that the data will be used as evidence in criminal or civil proceedings. In perhaps the great majority of cases, therefore, the only prospect for the review of a request for communications data – other than someone's entirely speculative complaint to the IPT[356] – will be the possibility of inspection by the Interception Commissioner and his team of inspectors.

166. However, the adequacy of this review appears to leave much to be desired. First, although public authorities have had the power to request communications data under RIPA since January 2004, it was not until late 2005 that the Home Office had recruited and trained the staff necessary to carry out inspections, as Sir Swinton Thomas explained in February 2007:[357]

> A recruitment exercise was undertaken through my sponsoring department, the Home Office. A recruitment agency was instructed, and there were a very large number of applicants. The applications had to be sifted and assessments made. This took a considerable time. Following the assessment, a number of applicants were interviewed by a panel of three, consisting of myself and two senior Members of the Home Office (the Head of my sponsor unit and an independent assessor). A Chief Inspector and five Inspectors were chosen, *all with relevant experience from working in law enforcement or the private sector of using or interpreting communications data in criminal investigations and proceedings.* The Chief Inspector was in post on 16 May 2005 and the remainder of the team joined between that date and 4 September 2005. Thereafter it was necessary for them to be trained in this work which included attendance at a residential course and the inspections commenced in the latter part of 2005.

Given, however, that RIPA was enacted in July 2000 and the relevant provisions were not brought into force for nearly four years, it was clearly unacceptable that there was no adequate inspection regime in place for at least a year and a half after public bodies gained the power to make requests. As Sir Swinton himself conceded, it would be 'impossible' for him to have undertaken this oversight work by himself.[358] Between 2004 and late 2005, therefore, there was plainly no effective review being carried out of communications data requests under RIPA.

167. Second, even with a team of inspectors in place, the sheer volume of requests – which average about half a million each year – makes it impossible for the Commissioner and his team to review anything more than a very small proportion of requests. This is particularly true given that the same inspection team also has responsibility for interceptions in prisons.[359]

168. Third, although the Interception Commissioner has identified a number of technical errors by public bodies in his annual reports over the years, neither he nor his inspectors appear to have ever reviewed a request for communications data made by a public body that they judged to have been unnecessary or disproportionate. Given that there have been probably somewhere close to three million requests made since January 2004, this suggests either a degree of effectiveness in

356. See Chapter 9 below.
357. 2005-2006 report, n251 above, para 10, emphasis added.
358. Ibid.
359. Ibid.

public body decision-making that approaches infallibility, or more likely, that the Commissioner's oversight is ineffective.

169. It is worth noting, for instance, that none of the inspectors appointed to assist the Interception Commissioner appear to have any legal or judicial qualifications, having been recruited from either law enforcement or the communications sector.[360] Although this suggests that the inspectorate has a considerable amount of operational and investigative expertise, it is unclear what, if any, expertise they have in assessing communications data requests on human rights grounds.[361] This is particularly worrisome when, for example, an inspection in 2009 identified 'serious failings and weaknesses' in the procedures used by some local authorities to request data:[362]

> Five of the local authorities did not emerge well from their inspections and serious failings and weaknesses were found in their systems and processes. *The applications submitted by four of these public authorities lacked detail and on their own did not adequately justify the principles of necessity and proportionality. However, my Inspectors discussed the investigations with the relevant staff and concluded that the acquisition of the data was justified…*

The fact that the inspectors do not appear to be particularly well-qualified to review the legality of requests by public bodies would appear to be less problematic given that they are supervised by the Interception Commissioner, who is a former Lord Justice of Appeal. Unfortunately, however, in his recent testimony before a parliamentary committee concerning the Protection of Freedoms Bill, the Interception Commissioner Sir Paul Kennedy himself displayed a surprisingly narrow approach to the issues of necessity and proportionality. In answer to questions about the use of communications data by local authorities, Sir Paul appeared to be unwilling to contemplate the investigation of low-level offences by less intrusive means:[363]

> ***Q121 Michael Ellis:*** Would you accept, Sir Paul, that there are other ways of detecting crime than the interception of communication? Would you accept that there are other democratic countries that detect crime by an alternative route?
>
> ***Sir Paul Kennedy:*** Sometimes, but often not. In relation to the type of work that I am concerned with — that is what we are talking about here, although it concerns a lot of other things — the fact is that, if you put yourself in the position of a householder, through the letterbox comes a card with a mobile number on it. It says, 'I will take away all that unwanted rubbish in your garden, just dial this number'. The rubbish is taken away and fly-tipped, and the only lead you have is the mobile number. If the Bill comes into effect, in order for a local authority to discover to whom that mobile number belongs it would have to go to a magistrate. So I do not think it is necessary.

360. See Chapter 3 above.
361. See Swinton Thomas, 2005-2006 report, n251 above, para 22: 'The objectives of the Inspectors are to ensure that communications data is being acquired in accordance with the Act and the Code of Practice, and *in particular to ensure that the principles of necessity and proportionality are being complied with,* and to ensure that relevant records are kept, that errors are reported, and that training is adequate. In this way independent oversight is provided and good and bad practice is identified and fed back into the inspection process'. Emphasis added.
362. Kennedy, 2010 report, (HC 1239, June 2011), para 7.43. Emphasis added.
363. Evidence of the Interception of Communications Commissioner, Sir Paul Kennedy, to the House of Commons Public Bill Committee on the Protection of Freedoms Bill, 22 March 2011.

> ***Q122 Michael Ellis:*** Would there not be alternative methods for discovering fly-tipping, such as witnesses or closed circuit television surveillance? There are alternative methods under your scope, are there not?
>
> ***Sir Paul Kennedy:*** No. Closed circuit television is nothing to do with my remit.

170. In other words, the Interception Commissioner's assessment of the proportionality of requests for communications data appeared to be skewed, consciously or otherwise, by the fact that various alternative means of investigation were outside his statutory remit. The possibility of investigating the fly-tipping by, for instance, phoning the number on the card and making enquiries does not appear to have occurred to the Commissioner. The tendency of public officials to assume that requesting access to private communications data is always the most effective route is something that judicial oversight is meant to check. It is, therefore, dismaying to see this attitude reflected in the Commissioner himself. Even more dismaying were the Commissioner's responses in the following exchange:[364]

> ***Q147 Tom Brake:*** I just wonder, Sir Paul, whether you have ever sat down with someone who has had the powers used against them and asked them whether they felt that it had been an abuse of power.
>
> ***Sir Paul Kennedy:*** The only sort of people whom it is used against is rogue traders.
>
> ***Q148 Tom Brake:*** Allegedly. You are confident that all 1,811 people who have been subject to these powers [by local authorities in 2010] fall into that category. You know that for a fact.
>
> ***Sir Paul Kennedy:*** They are not necessarily rogue traders, but they fall into the categories that I have defined, yes.
>
> ***Q149 Michael Ellis:*** Sir Paul, forgive me. You have been a lawyer for many years, I presume. Surely they are allegedly rogue traders until they are proven guilty. You are innocent until proven guilty.
>
> ***Sir Paul Kennedy:*** Of course. I entirely agree, *but on the other hand, if the number is given to us by a complaining member of the public* as the number on the card that was put through their door, *that is how we investigate it.*

Although the Interception Commissioner denied that he assumed the guilt of those who were the subject of communication data requests under RIPA,[365] the manner of his answers above tends to suggest otherwise. In particular, his use of the pronouns 'we' and 'us' indicates a degree of identification with the work of public authorities that is surely unhealthy in a judge charged with the independent review of their decisions. After all, neither the Commissioner himself nor his inspectors receive complaints from members of the public, nor do they investigate them,[366] so it is difficult to see how else he meant his answer to be understood.

---

364. Ibid.
365. Ibid, Q150.
366. See eg, ibid, Qs 144-146.

171. Certainly, Sir Paul's apparent conviction that public authorities only investigate wrongdoers goes some way to explaining how, despite almost three million requests for communications data having been made since 2004, no Interception Commissioner has ever found a single request to have been unnecessary or disproportionate. In the circumstances, therefore, it is difficult to regard his limited and somewhat one-sided oversight as either an adequate or effective check against disproportionate or unnecessary requests for communications data under RIPA.

Unnecessarily broad access

172. Although section 22 of RIPA requires that any individual request for data by a public body must be necessary and proportionate, the broader question of whether it is proportionate for an exceedingly wide range of public bodies to be able to make requests in the first place, often for the sake of investigating minor criminal or regulatory offences, has never been properly addressed. As the Newton Committee of Privy Counsellors reported in December 2003:[367]

The existence of data creates its own demand for access to it from a wide range of bodies for a variety of reasons, mostly unrelated to national security. It also creates the potential for abuse. It is, therefore, important to maintain strict limits on the Government's ability to require data to be retained and on the circumstances in which data can be accessed, and to ensure that the access rules are strictly enforced.

173. When RIPA was first enacted in July 2000, the only bodies able to request communications data were the police, the intelligence services, Inland Revenue and Customs and Excise.[368] By 2003, however, the government had proposed a massive extension of these powers to a wide range of public bodies. When Chapter 2 of Part 1 finally came into force in 2004, the number of bodies able to request data included more than 600 public bodies, including 100 NHS trusts and more than 300 local authorities.[369] Successive extensions in 2005 and 2006 meant that by the beginning of 2007, a total of 795 public bodies were able to request communications data under RIPA.[370]

174. There was widespread public outcry over the use of surveillance powers under RIPA by local authorities in 2008, following the discovery that Poole Borough Council authorised directed surveillance against a family of four alleged to be sending their children to school out-of-zone.[371] In January 2009, the House of Lords Constitution Committee issued its report on surveillance powers, expressing concern at 'the use by some local authorities of their surveillance and communication data collection powers under RIPA', and recommending that the government consider 'whether local authorities, rather than the police, are the appropriate bodies to exercise such powers'.[372] The following month, the Home Office issued a consultation that proposed limiting the number of public authorities able to make requests.[373] This was followed in turn by a statutory instrument in February 2010 that stripped several bodies of the power to request communications data. However,

367. See n332 above, para 398, emphasis added.
368. Section 25(1). See eg, the statement of the Home Secretary Jack Straw that the RIPA provisions on communications data were meant to apply to the activities of 'the law enforcement, security and intelligence agencies', that the purposes for which information could be sought were broadly similar to that under existing legislation and that, 'as a result, I do not expect any significant change in the extent to which communications data are obtained' (Hansard, HC Debates col 509W, 19 April 2000.
369. See SI 2003/3172, 2005/1083 and 2006/1878.
370. Swinton Thomas, 2005-2006 report, para 8.
371. See eg, BBC News, 'Council admits spying on family', 10 April 2008.
372. N72 above, para 177.
373. Home Office, *Regulation of Investigatory Powers Act: Consolidating Orders and Codes of Practice* (April 2009).

the remaining bodies still included all local authorities and NHS trusts as well as hundreds of other public bodies. Consequently, following the 2010 General Election, the Coalition Programme for Government promised to:[374]

> ban the use of powers in the Regulation of Investigatory Powers Act (RIPA) by councils, unless they are signed off by a magistrate and required for stopping serious crime.

175. In June 2010, the Home Secretary ordered the Home Office to undertake an urgent review of counter-terrorism powers, which included examination of:[375]

> the question of access to communications data by public authorities more generally, in addition to the specific commitment in relation to local authorities. The purpose of this work would be *to tighten the safeguards on the acquisition and handling of communications data and ensure that any intrusion into privacy is clearly demonstrated to be necessary.*

In its report back in January 2011, the Home Office review noted that the government had already committed to 'rationalise the legal bases by which communications data can be acquired and, as far as possible, to limit that to RIPA'[376] as well as:[377]

> stop local authority use of RIPA (Regulation of Investigatory Powers Act 2000) *unless it is for serious crime and approved by a magistrate:* local authorities have been criticised for using covert surveillance in less serious investigations including, for example, dog fouling or checking an individual resides in a school catchment area.

As Lord Macdonald of River Glaven QC, the former DPP, noted in his parallel report on the review, there was 'a good deal of public and media concern in recent years' that the use of RIPA powers by local authorities 'has been excessive and inadequately policed'.[378] Certainly, he noted, the evidence gathered by the Review 'appears to indicate that confidence in the processes is low'.[379]

176. Consequently, clause 37 of the Protection of Freedoms Bill published in February 2011 has proposed amending section 23 of RIPA to require prior judicial authorisation for requests by local authorities to access communications data. Specifically, it requires that any authorisation or notice issued by a designated person under Chapter 2 of Part 1 will not take effect unless and until a magistrate has, among other things, satisfied himself that it was necessary and proportionate to do so. Notably, clause 23A(6) would give the Secretary of State the power to make regulations extending the requirement to obtain judicial approval for requests to *any other* public authority.

177. In his evidence to the House of Commons on the Protection of Freedoms Bill, the Interception Commissioner was strongly critical of these provisions, describing them as 'wholly unnecessary' given the relatively small number of requests made by local authorities, the corresponding cost of judicial authorisation,[380] and the absence of any evidence of abuse.[381] The Commissioner is correct

374. Coalition programme for government, n74 above, p12.
375. N349 above, p28. Emphasis added.
376. Ibid, p5.
377. Ibid, p25.
378. N335 above, p6.
379. Ibid, p6.
380. Evidence of the Interception of Communications Commissioner, Sir Paul Kennedy, to the House of Commons Public Bill Committee on the Protection of Freedoms Bill, 22 March 2011, Q107.
381. Ibid, Q111.

to note that local authorities in fact make up only a tiny fraction of requests for communications data. Whether the cost of judicial authorisations is excessive, however, depends on your view of whether it is a necessary safeguard against abuse. As to the evidence of abuse itself, though, there is clearly some cause to doubt the Commissioner's somewhat sanguine assessments for the reasons set out in the previous section.

178. In any event, the Commissioner's criticisms reveal an inadequate understanding of the principle of proportionality in the context of surveillance. There is, after all, an inherent risk in any criminal investigation involving intrusive surveillance that the resulting invasion of privacy will in hindsight prove to have been unnecessary because the initial suspicion turns out to be false: what Lord Neuberger described as one of the paradoxes of surveillance.[382] This inherent risk can be minimised by, for example, requiring that less intrusive means be considered first, but it can never be eliminated.

179. Whether it is proportionate, therefore, to run the risk of invading someone's privacy in the knowledge that they may turn out to be innocent depends on several factors, including the reasonableness of the suspicion *but also* the seriousness of the offence in question. It is the difference, in other words, between breaking down the door to someone's hotel room because you think they are being murdered, and breaking down the door to their hotel room because you think they have stolen your toothbrush. In both cases, your suspicion may be very well-founded but there is also an inevitable risk that you are mistaken. And should it turn out that you are mistaken, the reasonableness of your suspicion will be of little comfort to the person whose privacy you have unnecessarily invaded. But at least in the case of suspected murder, we would say that the seriousness of the suspected offence, combined with the reasonableness of your suspicion, helped to excuse your actions. The same could not be said of the toothbrush.

180. The seriousness of the suspected offence as a factor in assessing the proportionality of a surveillance decision was recognised in the recent decision of the Strasbourg Court in *Uzun v Germany*.[383] In that case, the Court had regard to the fact that the investigation 'for which the surveillance was put in place *concerned very serious crimes*, namely several attempted murders of politicians and civil servants by bomb attacks'.[384] Noting that the German police had already tried less intrusive means which had been thwarted by the suspect, the Court found the use of GPS data to be plainly justified.[385] But the fact that it had regard to the seriousness of the offences involved, as well as to the availability of less intrusive means, points very strongly towards the likelihood of the Court reaching a different decision in a case involving very minor criminality, eg, suspected fly-tipping, in which the authorities had other means open to them for obtaining the same information, as they will inevitably have in such cases.

181. This is not to say that minor offences like fly-tipping are undeserving of investigation. Rather, it is that the harm involved in most minor offences is, by definition, insufficiently serious to justify the inherent risk that surveillance poses to the privacy of any person who falls under suspicion. In almost every case, less intrusive forms of investigation are likely to be an equally effective and, therefore, more proportionate means of investigating minor crimes than the resort to surveillance powers.

382. *In re McE* [2009] UKHL 15 at para 111.
383. See n174 above.
384. Ibid, para 80. Emphasis added.
385. Ibid.

Increasingly intrusive nature of communications data

182. One problem associated with the increasing use of communications data requests by public bodies is the increasingly intrusive nature of the data itself, particularly in relation to Internet usage. As the Information Commissioner has noted, 'communication records … can be highly intrusive even if no content is collected. You can tell an awful lot about some people's personal circumstances from the people they are talking to and the websites they visit'.[386]

183. Moreover, as a group of academics in the Information Systems and Innovation Group of the London School of Economics noted in their 2009 briefing on the government's Interception Modernisation Programme,[387] the distinction between so-called 'traffic data' relating to Internet use, on the one hand, and the actual interception of the contents of a communication, on the other, is becoming increasingly blurred, particularly by the use of deep packet interception:[388]

> [W]ith Internet technology you have to collect everything and then throw away what the law does not allow you to have or use. We think that at a practical level the communications data/intercept distinction will be impossible to intercept both for ISPs and the courts. Moreover, the existing balance of protections against abuse will also be lost.

So, for instance, the distinction between the traffic data of a phone call made on a landline (which number was called, when and for how long), and the content of that call (what was said) is relatively clear cut. When it comes to accessing the traffic data of a person's Internet session, however, the very way in which the data is obtained is likely to disclose much of what we would consider to be the *content* of the communication. As a result, it will often be much easier and equally probative for authorities to self-authorise a request for traffic data concerning someone's Internet use than to obtain an interception warrant for the same Internet session.

184. The failure of the law to keep pace with the increasing pace of technological change is also evident when it comes to traditional assessments of the intrusion caused by the use of location data. In the 1984 decision of *Malone*, for instance, although the Court noted the interference with privacy caused by the Post Office's metering of Malone's phone calls, allowing them to see which numbers he had called, when and for how long, it was also clear that this was less of an intrusion than the monitoring of the *content* of his phone calls.[389] Similarly, in the 2010 case of *Uzun*, the Court was concerned with the intrusion caused by a GPS locator that had been planted in the car of an associate of the suspect.[390] Among other things, it noted that GPS surveillance was:[391]

> by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings.

386. Information Commissioner's statement on the Communications Data Bill, 27 April 2009.
387. LSE Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (June 2009).
388. Professor Peter Sommer of the Information Systems and Innovation Group quoted in the LSE press release, 'Home Office Internet surveillance proposals won't work says LSE study', 17 June 2009.
389. See n124 above.
390. See n174 above.
391. Ibid, para 52.

Although this was true in the particular facts of Uzun's case – chiefly because the locator could only track his movements when in his associate's car – it certainly does not hold true for access to location data in general. Given that more than 80 per cent of adults in the UK now regularly carry a device that transmits its location from moment to moment, often with considerable accuracy, ie, a mobile phone,[392] it is clear that access to the location data of a person's phone is likely to disclose far more information concerning their conduct than the now-antiquated meter that the Post Office attached to Mr Malone's phone line in the late 1970s.

185. The intrusive nature of location data was recently underlined by allegations published in July 2011 that reporters from the *News of the World* regularly paid police £300 per request to 'ping' the location of mobile phones belonging to celebrities and public figures.[393] Although Part 4 of RIPA allows people who suspect their communications have been wrongly requested by a public authority to complain to the IPT, the Tribunal has no power to investigate the unlawful accessing of communications data by private companies or individuals unless a public body is alleged to have been involved as an intermediary. Investigating the alleged unlawful disclosure of personal data by private companies is otherwise a matter for the Information Commissioner.

186. For its part, the government has claimed that the changing nature of communications technology has degraded its own ability to access relevant data. As the Home Office website complains:[394]

> Much of our current capability is based on an era of fixed and mobile telephones and was not designed to deal with the growth in the use of the Internet. With Internet service providers often based abroad, and fewer communications being itemised for billing purposes, investigative capability is declining.

For this reason, the government previously sought to introduce a Communications Data Bill in 2008 that would have, among other things, required communications service providers to give police and intelligence agencies unprecedented access to their networks for the purposes of facilitating interceptions and requesting data. This was subsequently withdrawn in the face of widespread opposition: the former Director of Public Prosecutions Sir Ken Macdonald QC, for instance, described the proposals as seeking to create 'an unimaginable hell-house of personal private information'.[395] However, the Coalition government has indicated that it may yet legislate to upgrade the capabilities of law enforcement and the intelligence services in this area. In its Strategic Review published in October 2010, the government committed itself to 'introducing a programme' to:[396]

> preserve the ability of the security, intelligence and law enforcement agencies to obtain communication data and to intercept communications within the appropriate legal framework. This programme is required to keep up with changing technology and to maintain capabilities that are vital to the work these agencies do to protect the public. Communications data provides evidence in court to secure convictions of those engaged in activities that cause serious harm. It has played a role in every major Security Service counterterrorism operation and in 95% of all serious organised crime investigations.

392. See eg, Adrian Shepherd, *Use of ICT among Households and Individuals* (Office for National Statistics, 2007).
393. See the *New York Times,* 'Murdoch Tabloid's Targets Included Downing Street and the Crown', 11 July 2011; 'Phone hacking: Met police to investigate mobile tracking claims', the *Guardian,* 21 July 2011.
394. See www.homeoffice.gov.uk/counter-terrorism/communications-data/
395. See 'Private firm may track all email and calls' by Richard Norton-Taylor and Alan Travis, the *Guardian,* 31 December 2008.
396. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948, October 2010), p44.

However, the government also promised to legislate in order to 'put in place the necessary regulations and safeguards' that would 'ensure that our response to this technology challenge is compatible with the Government's approach to information storage and civil liberties'.[397]

The riots and social media

187. Following the riots in early August, considerable public attention was paid to the ability of police to access communications data for the sake of preventing and detecting crime. In his statement to Parliament following the riots, for instance, the Prime Minister David Cameron said that 'everyone watching these horrific actions will be struck by how they were organised by social media', and said that the government was working with the police and intelligence services to look at:[398]

> whether it would be right to stop people communicating via these websites and services *when we know* they are plotting violence, disorder and criminality.

On the same day as the Prime Minister's statement, the Home Secretary also gave a speech in Parliament in which she similarly claimed that 'sites like Facebook and Twitter and messaging services like Blackberry Messenger have been used to coordinate criminality, and stay one step ahead of the police'.[399] She promised to convene a meeting with the Association of Chief Police Officers (ACPO), the police and social media representatives 'to work out how we can improve the technological and related legal capability of the police', including 'whether and how we should be able to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality'.

188. Following the meeting, which was held on 25 August, the government appeared to retreat from its earlier plans to block access to social media during public unrest,[400] particularly as subsequent analysis of the traffic on sites such as Twitter during the course of the riots showed 'little immediate evidence that the social network was used to orchestrate disorder'.[401] However, the *New York Times* reported Gordon Scobbie, the Deputy Chief Constable of Tayside Police and the ACPO lead on digital engagement, as saying that 'the group had discussed how far the networks might be willing to bend privacy rules to assist the police in pursuing online criminal activity'.[402]

189. We see no reason, however, for 'privacy rules' to be bent by communication service providers or the police themselves. Existing powers under RIPA for the request of communications data are more than broad enough to enable the police to investigate the conduct of suspected rioters. Indeed, just as the sentencing guidelines appear to have been disregarded by magistrates in recent weeks,[403] we are concerned that there is an even greater risk than usual of police and other public bodies making unnecessary or disproportionate requests for communications data – something the weak safeguards offered by RIPA are likely to do little to prevent or restrain.

397. Ibid.
398. PM statement on disorder in England, 11 August 2011. Emphasis added.
399. Theresa May: speech on riots, 11 August 2011.
400. See eg, 'Home Office backs away from social network blocking after riots', by Tim Bradshaw, the *Financial Times,* 25 August 2011.
401. 'Riots database of 2.5m tweets reveals complex picture of interaction' by James Ball and Paul Lewis, the *Guardian,* 24 August 2011.
402. 'In Britain, a Meeting on Limiting Social Media' by Ravi Somaiya, the *New York Times,* 25 August 2011.
403. See eg, 'Magistrates were told to send rioters to the Crown Court, emails show', the *Guardian,* 14 September 2011.

Recommendations

Introduce and extend the use of prior judicial authorisation

190. Although it is true that requesting access to someone's communications data is generally less intrusive a means of surveillance than the interception of their communications, this does not mean that it cannot be intrusive at all. As noted above, there are a number of circumstances in which the intrusion can be as severe as that posed by interception. This is especially true given the increasing amount of data that is available in relation to digital communications, and the increasingly blurred distinction between traffic data and content in the context of requests for data on Internet usage.

191. Accordingly, we recommend that the provisions of the Protection of Freedoms Bill requiring prior judicial authorisation of communications data requests by local authorities be introduced and extended to all other public bodies, except in the case for requests for subscriber data by the police, law enforcement, the intelligence services and the emergency services. These latter bodies would require prior judicial authorisation to obtain traffic data and service use data in the usual way. However, this should be accompanied by a power for the same bodies to request traffic data and service use data without prior judicial authorisation in cases of emergency, to be followed by judicial confirmation within 48 hours.

192. We also recommend that the model of authorisation and prior judicial approval as currently set out in the Protection of Freedoms Bill should be replaced by a more straightforward process of the relevant public authority applying directly to the magistrate for a communications data warrant.

193. In addition, all existing restrictions on public bodies to obtain any kind of data that they cannot currently obtain should also be retained, eg, even if prior judicial authorisation were introduced, local authorities still should not be able to request traffic data for instance.

Reduce the number of public bodies with access to communications data

194. Consistent with our view set out above that warrants should be required in order for any public body to obtain traffic data and service use data, and in order for non-law enforcement bodies in respect of requests for subscriber data, we also recommend that the number of public bodies that have the power to request such data in the first place should be restricted to only the emergency services (who generally use their power to obtain communications data in order to locate people during emergencies), the intelligence services, and those agencies with responsibility to investigate serious criminal activity. In particular, we agree with the threshold proposed by the House of Commons Constitution Committee in its 2009 report into surveillance power, ie, 'the investigation of serious criminal offences that would attract a custodial sentence of at least two years'.[404]

195. We also urge the government to continue its current work to rationalise the 'wealth' of different statutory powers that public bodies have to request communications data outside of RIPA, in order to ensure that 'RIPA is the only mechanism by which communications data can be acquired'.[405]

404. See n72 above, para 177.
405. See n349 above, p29.

Improve independent oversight

196. We have identified a number of concerns with the quality of oversight provided by the Interception Commissioner and his team of inspectors. As with the introduction of prior judicial authorisation for interceptions, we believe that having a judge decide whether access to communications data is necessary and proportionate is likely to radically reduce the oversight burden on the Interception Commissioner's office.

197. More generally, although we generally favour the establishment of a single oversight regime as far as possible, we consider that the kind of issues raised by the use of communications data by local authorities (eg, straightforward requests for access to subscriber data) are likely to be different in kind from those raised by the work of law enforcement and intelligence bodies, particularly the use of traffic data.

198. We, therefore, propose that the oversight work of the Interception of Communications Commissioner in relation to communications data should be divided up between the Surveillance Commissioners and the Information Commissioner. The former would take responsibility for oversight of requests for data by the police, the intelligence services, and other national law enforcement bodies. The latter would take responsibility for oversight of requests for communications data by all other, non-law enforcement bodies such as local authorities, fire and ambulance services.

199. This is because, in our view, the Information Commissioner is better placed to oversee low-level requests in relation to the relatively low number of requests that come from non-law enforcement bodies, such as the Trading Standards Service, whereas the Chief Surveillance Commissioner is better placed to oversee the requests in relation to the investigation of serious crime and threats to national security, etc.

Chapter 5
'Intrusive' surveillance

200. At its Second Reading in the House of Commons in December 1988, the Bill that became the Security Service Act 1989 was described by one MP as a 'chip to appease the European Court of Human Rights'.[406] This was a reference to the Court's first-instance body, the European Commission on Human Rights, which in May that year had given an admissibility ruling in the case of *Harman and Hewitt v United Kingdom*. Although better known today as two former cabinet ministers, both applicants had previously worked at Liberty where – it was revealed by a whistleblower in 1985 – they had been the subject of MI5 surveillance.

201. Less than two weeks after the 1989 Act was passed, the Commission gave its final decision, ruling that the surveillance of the applicants, together with the absence of a legal framework that indicated 'with the requisite degree of certainty the scope and manner of the exercise of discretion by the Security Service' when carrying out surveillance, meant that the government was in breach of Article 8(2).

202. Under the 1989 Act, MI5 was put on a statutory footing for the first time and section 5 in particular made provision for the Secretary of State to issue warrants for authorising entry on or interference with property or with wireless telegraphy, eg, for the planting of surveillance devices, where he believes it is necessary to obtain information 'likely to be of substantial value' to MI5 and which 'cannot reasonably be obtained by other means'.[407] It also established the office of the Security Services Commissioner to oversee its activities.[408]

203. This was followed by the Intelligence Services Act 1994, which put MI6 and GCHQ on a similar footing as MI5. It replaced the Commissioner and Tribunal under the 1989 Act with the Intelligence Services Commissioner and the Intelligence Services Tribunal to respectively provide oversight of, and hear complaints against, all three services.[409] In addition, it established the Security and Intelligence Committee to provide for broader oversight of the 'expenditure, administration and policy' of the intelligence services.[410] It also made general provision for warrants for all three agencies on similar terms as that provided by the 1989 Act,[411] lasting six months where signed by

406. Jonathan Aitken MP, Hansard HC debates col 1133, 15 December 1998. See also David Winnick MP at the Bill's Third Reading, col 777, 23 January: ' I wonder whether we would have such a Bill if it had not been for the complaint brought by my hon. Friend the Member for Peckham (Ms Harman) and Patricia Hewitt to the European Court of Human Rights'.
407. Section 3(2).
408. Section 4.
409. Sections 8 and 9.
410. Section 10.
411. Section 5(2).

the Secretary of State or two working days where signed with his authorisation on an urgent basis by a senior official.[412]

204. In the 1996 case of *R v Khan*, which concerned the admissibility of evidence obtained from a police bug planted in the defendant's friend's flat, Lord Nolan said:[413]

> The sole cause of this case coming to your Lordships' House is the lack of a statutory system regulating the use of surveillance devices by the police. The absence of such a system seems astonishing, the more so in view of the statutory framework which has governed the use of such devices by the Security Service since 1989, and the interception of communications by the police as well as by other agencies since 1985.

As noted above, this led to the passing of the Police Act 1997, Part 3 of which provides for a senior member[414] of the police, the National Crime Squad, the National Criminal Intelligence Unit, and HM Revenue & Customs to authorise interference with property or wireless telegraphy,[415] where he believes it is both necessary for the prevention and detection of crime and proportionate to 'what the action seeks to achieve'.[416]

205. At the same time, Part 3 of the 1997 Act also established the office of the Surveillance Commissioners – required by section 91(2) to be 'persons who hold or have held high judicial office' – to approve any authorisation that concerns property believed to be:[417]

i. a person's dwelling;
ii. a hotel bedroom; or
iii. an office.

Or any authorisation likely to result in 'any person acquiring knowledge of':[418]

i. matters subject to level privilege;[419]
ii. confidential personal information;[420] or
iii. confidential journalistic material.[421]

Approval by a commissioner is not required, however, 'where the person who gives it believes that the case is one of urgency'.[422] Authorisations last three months, other than urgent authorisations given orally which lapse after three days.[423] The Commissioner also has the power to quash any authorisation where he is satisfied that, at the time it was given or renewed, 'there were no reasonable grounds for believing' it was necessary or proportionate to do so,[424] including any

412. Sections 6(1) and (2).
413. See n111 above.
414. As defined in section 93(5). Section 96, however, provides for urgent authorisations in the absence of the relevant person.
415. Section 93 of the Police Act 1997.
416. As amended by section 75(4)(b) of RIPA. The original language of section 93(2)(b) provided that the authorising officer must believe that 'what the action seeks to achieve cannot be reasonably achieved by other means'.
417. Section 97(2)(a).
418. Section 97(2)(b).
419. Section 98.
420. Section 99.
421. Section 100.
422. Section 97(3).
423. Section 95(2).
424. Section 103(1).

authorisation that ought to have required a Commissioner's approval due to its intrusiveness.[425] The Act also provides for agencies to appeal against a Commissioner's decision to the Chief Surveillance Commissioner.[426]

206. However, the provisions in the 1994 Act (governing property interference by the intelligence services) and the 1997 Act (governing property interference by police) did not refer in terms to the use of surveillance techniques that did not necessarily involve interference with property but were nonetheless highly intrusive, eg, planting a listening device in a prison cell to listen to a suspect's private consultation with his solicitor or conducting covert video surveillance of someone's bedroom from a public place.

207. In light of the long line of judgments from the Strasbourg Court concerning the need to regulate surveillance powers, the absence of any statutory framework to cover the full range of methods that might be deployed by police or intelligence agencies was very obviously contrary to the requirements of Article 8(2). With the HRA 1998 due to come into force on 2 October 2000, the government, therefore, took the opportunity to develop a comprehensive statutory scheme for the regulation of surveillance powers (albeit one that was, in fact, the crude knitting together of several pre-existing schemes with the development of some new ones).

208. Part 2 of RIPA governs the use of three key surveillance techniques: 'intrusive' surveillance, 'directed' surveillance, and covert human intelligence sources. The latter two are dealt with in Chapters 6 and 7 respectively. This Chapter looks at the use of so-called 'intrusive' surveillance under Part 2 of RIPA and the Code of Practice on Covert Surveillance and Property Interference.

209. First, it is important to note that, although the purpose of Part 2 is to make authorised surveillance 'lawful for all purposes',[427] it does *not* follow from this that surveillance that has not been authorised under Part 2 is thereby unlawful. As the Chief Surveillance Commissioner pointed out in a recent report, 'the absence of an authorisation does not prevent the use of covert surveillance'.[428] A failure to obtain authorisation might give rise to a challenge to the admissibility of any evidence acquired as a result under section 78 of the Police and Criminal Evidence Act (PACE), although this would obviously have no bearing on surveillance which was only carried out for intelligence purposes, etc. Failure to obtain authorisation would also, in principle, give rise to a claim under sections 6 and 7 of the HRA for breach of Article 8 ECHR. This would generally require, however, the person affected being aware of both the surveillance and its lack of authorisation in the first place. In any event, the IPT has exclusive jurisdiction over any HRA claims in respect of Part 2.[429]

210. 'Surveillance' in Part 2 is generally defined as:[430]

a) monitoring, observing or listening to persons, their movements, their conversation or their other activities or communications;

b) recording anything monitored, observed or listened to in the course of surveillance; and

425. Section 103(2).
426. Section 104.
427. Section 27(1).
428. Sir Christopher Rose, *Annual Report of the Chief Surveillance Commissioner 2009-2010* (HC 168, July 2010), para 5.21.
429. Sections 65(2)(a) and (5)(d).
430. Section 48(2).

c) surveillance by or with the assistance of a surveillance device.

However, 'surveillance' under Part 2 does *not* include:

a) the use of a covert human intelligence source to obtain or record any information (whether or not using a surveillance device) which is disclosed in the presence of the source;[431]

b) entry on or interference with property or wireless telegraphy that would otherwise fall to be authorised under Part 3 of the Police Act 1997 or under the Intelligence Services Act 1994;[432] or

c) interception of a communication without a warrant where one of the parties consents to the interception (eg, knows that the call is being recorded).[433]

211. 'Intrusive' surveillance is exhaustively defined under Part 2 as surveillance that is both 'covert' (ie, 'carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place')[434] *and*:

a) 'carried out in relation to anything taking place on any residential premises (including temporary residences such as hotels or prisons, but excluding their common areas such as hotel dining rooms, prison canteens or police interview rooms);[435] or

b) in any private vehicle (including business vehicles such as work vans or company cars);[436]

And either:

a) involves the presence of an individual on the premises or in the vehicle;[437] *or*

b) is carried out by means of a surveillance device present on the premises or in the vehicle;[438] or

c) is carried out by means of a surveillance device that is not present on the premises or in the vehicle but consistently provides information of the same quality and detail as might be expected to be obtained from a device that was.[439]

However, surveillance that falls within the above definition will *not* count as 'intrusive' to the extent that:

a) it is carried out exclusively by means of a surveillance device 'designed or adapted principally for the purpose' of tracking the vehicle's location;[440] *or*

431. Section 48(3)(a) and (b).
432. Section 48(3)(c).
433. Section 48(4).
434. Section 26(9).
435. Sections 48(1) and (7) and para 2.13 of the Code of Practice.
436. Section 26(3) and para 2.17 of the Code of Practice.
437. Section 26(3)(a).
438. Sections 26(3)(b).and 26(5).
439. Ibid.
440. Section 26(4)(a).

b) it involves interception without a warrant where one of the parties has consented to the interception.[441]

Following the judgments of the Divisional Court in *In re C*[442] and the House of Lords in *In re McE*[443] in 2007 and 2009 respectively, the definition of 'intrusive' was supplemented by the Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010,[444] which provides that directed surveillance of legal consultations carried out in police stations, prisons, lawyers' offices, courts, or any other place in which people may be held in custody or detention shall be treated as intrusive surveillance.[445]

212. The definition of 'intrusive' surveillance is meant to ensure that activities under Part 2 of RIPA that involve serious interference with privacy are subject to a higher standard of authorisation than other, less intrusive forms of surveillance. Whether in fact the definition and authorisation procedures are adequate to this purpose, however, is discussed below. It is also worth noting that authorisations for intrusive surveillance are frequently used by the police to by-pass the ban on intercept evidence in section 17 of RIPA by using a covert surveillance device to record the private phone conversations of suspects, which are then admissible as evidence in open court.[446]

213. Section 32 of RIPA provides that authorisation for intrusive surveillance may be given by either the Secretary of State or a senior authorising officer, ie, a chief constable of a police force, the Director General of SOCA, a designated Revenue and Customs official or the chairman of the Office of Fair Trading.[447] Authorisation may not be given unless the Secretary of State or senior authorising officer believe that the intrusive surveillance is necessary and proportionate, in the interests of national security, the prevention or detection of *serious* crime or the economic well-being of the UK.[448] In urgent cases, authorisation may be given by a senior officer's designated deputy.[449] Given the obvious overlap between authorisations for property interference under the Police Act 1997 and Intelligence Service Act 1994, on the one hand, and authorisations for intrusive surveillance under Part 2 of RIPA on the other, RIPA provides for combined authorisations to be given.[450]

214. Section 36 requires that any authorisation for intrusive surveillance made by the police, SOCA, Revenue & Customs or the OFT must be approved by a Surveillance Commissioner before it can take effect, unless the authorising officer has notified the Commissioner that it is a matter of urgency.[451] In addition, the Surveillance Commissioner has the power to quash or cancel an authorisation

441. Section 26(4)(b).
442. [2007] NIQB 101.
443. [2009] UKHL 15.
444. SI 461/2010.
445. Ibid, para 3(1).
446. See eg, *R v E* [2004] EWCA Crim 1243, in which the police recorded the accused's conversations for more than a month using a covert listening device placed in his car under a joint authorisation for property interference and intrusive surveillance. This included a number of phone conversations, which the Criminal Division of the Court of Appeal ruled were admissible on the grounds that 'what was recorded here was what happened independently of the operation of the telecommunications system' (para 22). The Court commented obiter that even a covert recording of both sides of a phone conversation transmitted by a hands-free device would not necessarily be inadmissible: ''Mr Meeke submits that, if that is so, devices may exist which are capable of picking up the contents of both ends of the telephone without there being interception and thus without the need for a warrant from the Secretary of State. We do not know whether that is so or not. We observe that even if it is, that would not mean that a device which overheard one end of a call that was being put through a loud speaker such as a speakerphone or handsfree set with loud speaker attached thereby became an intercepting device. That conclusion is consistent with the view frequently taken in cases before this Court and the House of Lords' (para 23).
447. Section 32(6). 'Serious' crime is defined in subsections 81(1) and (2) as an offence normally attracting a sentence of at least three years imprisonment, or which involves the use of violence, results in substantial finacial gain, or involves organised crime.
448. Section 32(3). Section 32(3A) further stipulates that the OFT may only seek intrusive surveillance for the sake of investigating cartel offences under section 188 of the Enterprise Act 2002.
449. Section 34.
450. See section 33(5).
451. Sections 35(2) and 36(3)(b). Where this is the case, the authorisation takes effect from the time it is granted.

where he is satisfied respectively that there were no reasonable grounds for believing that it was necessary and proportionate,[452] or that there are no longer reasonable grounds for believing it to be so.[453] He also has the power to quash an authorisation made under urgency where he is satisfied that there were no reasonable grounds for believing that the case was urgent.[454] Any ruling of a Surveillance Commissioner concerning an authorisation may be appealed by the senior authorising officer to the Chief Surveillance Commissioner.[455]

215. Section 41, by contrast, allows the Secretary of State to authorise intrusive surveillance on the application of the intelligence services, the Ministry of Defence, or HM forces. Section 42 provides that authorisation for intrusive surveillance by the intelligence services must be made under warrant.[456]

216. Authorisations for intrusive surveillance last for three months but can be renewed. Urgent authorisations, by contrast, last three days.[457]

217. Oversight of the use of intrusive surveillance is split between the Chief Surveillance Commissioner (in relation to authorisations by the police, SOCA, Revenue & Customs, and the OFT) and the Intelligence Services Commission (in relation to authorisations by the Secretary of State on behalf of the intelligence services, the Ministry of Defence, and HM forces), both of whom make annual reports concerning their activities.

218. Part 2 of RIPA came into force on 25 September 2000. Since that time, there have been 4,096 authorisations for intrusive surveillance by law enforcement bodies.[458] It is unclear, however, whether this is the number of authorisations that have been approved by the Surveillance Commissioners or simply the number of authorisations made by a senior authorising officer. If it is the latter, no figures are available for how many of these authorisations have subsequently been refused by the Surveillance Commissioners. Similarly, there are no statistics available to show the number of appeals by authorising officers against a Commissioner's decision, and the success rate of these appeals before the Chief Surveillance Commissioner.

219. In the same period as RIPA has been in force, 24,790 authorisations have been made for property interference under Part 3 of the Police Act 1997, including 1699 dwellings, 378 offices, and 403 hotel bedrooms.[459] RIPA makes provision for combined applications for authorisation for property interference under the Police Act and intrusive surveillance under Part 2. Although intrusive surveillance does not necessarily involve interference with property, it seems reasonable to infer that the great majority of authorisations for intrusive surveillance are accompanied by authorisations for property interference.

220. The number of authorisations for property interference quashed by the Surveillance Commissioners is extremely low: the highest number of authorisations quashed in any one year was 13 in 2009-2010;[460] the average is about five a year. However, these figures are high when compared with the

452. Section 37(2).
453. Section 37(3).
454. Section 37(4).
455. Section 38.
456. Section 42(1).
457. Section 43(c).
458. Source: annual reports of the Chief Surveillance Commissioner from 2000-2011.
459. Ibid.
460. *Annual Report of the Chief Surveillance Commissioner 2009-2010* (HC 168, July 2010), para 4.4.

number of authorisations for intrusive surveillance that have been quashed since 2000: a reported total of seven, of which all but two were quashed in 2010-2011 alone.[461]

221. In contrast to the detailed statistics available in the annual reports of the Chief Surveillance Commissioner, the number of authorisations made by the Secretary of State on behalf of the intelligence services – whether for intrusive surveillance or interference with property – has never been made public.

Lack of judicial control of authorisations by Secretary of State

222. In many ways, the role of Surveillance Commissioners in relation to authorisations for intrusive surveillance under Part 2 serves as a model for how most other parts of RIPA ought to function. It is the one part of RIPA in which the principle of prior judicial authorisation of surveillance powers operates on a daily basis, at least in the context of law enforcement. In cases of urgency where there is not time to obtain prior approval of a Commissioner, Part 2 sensibly allows for the police and agencies to self-authorise intrusive surveillance: such authorisations last only three days and can be cancelled or quashed by a Commissioner at any time.

223. The need for prior judicial approval of intrusive forms of surveillance was made particularly plain in the 2007 ruling of the Northern Irish Divisional Court, in which it held that the covert recording of a suspect's privileged conversations with his solicitor at a police station without judge's approval breached Article 8 ECHR.[462] This part of the Divisional Court's ruling was subsequently affirmed by the House of Lords in 2009.[463]

224. In addition to this basic safeguard of prior judicial control, the admissibility of any evidence that arises from intrusive surveillance – whether authorised or unauthorised – can also be challenged in any subsequent proceedings as evidence unfairly obtained.[464]

225. The same cannot be said, unfortunately, for the continuing role of the Secretary of State in authorising intrusive surveillance under Part 2 on behalf of the intelligence services, as well as warrants for property interference under the Intelligence Services Act 1994. Not only is the purpose of such surveillance the gathering of intelligence rather than evidence and, therefore, almost certain to escape the supervision of the ordinary courts, but – as with the interception of communications – the Secretary of State is insufficiently independent of his subordinates, both structurally and in terms of his sympathies, to act as an adequate or effective check against unnecessary or disproportionate authorisations for intrusive surveillance.

226. Just as the Interception of Communications Commissioner has repeatedly testified to the diligence of the Secretary of State in relation to the issuing of interception warrants, however, so too has the Intelligence Services Commissioner defended the Secretary of State's role in relation to the use of intrusive surveillance warrants under Part 2, indeed often using identical language. Consider, for example, the defence offered by the Intelligence Services Commissioner Lord Brown of Eaton-

461. *Annual Report of the Chief Surveillance Commissioner 2010-2011* (HC 1111, June 2011), para 4.5.
462. *In re C,* n442 above.
463. *In re McE,* n443 above.
464. See eg, section 78 of PACE in criminal proceedings and CPR 32.1 in civil proceedings.

Under-Heywood in his report for 2005-2006 and that given by the Interception Commissioner Sir Swinton Thomas in his own report for the same period. Lord Brown wrote:[465]

> Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity or proportionality are not met. The agencies are fully cognisant of the fact that the Secretary of State does not act as a 'rubber stamp'.

While Sir Swinton wrote:[466]

> Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity or proportionality are not met, and the agencies are well aware that the Secretary of State does not act as a 'rubber stamp'.

227. There is, similarly, a considerable degree of recycling in the reports of successive Intelligence Service Commissioners. In his outgoing report for 2005-2006, for instance, Lord Brown wrote:[467]

> In issuing warrants and authorisations the respective Secretaries of State must largely rely on the accuracy of the information contained in the application and the candour of those applying for it. This depends essentially upon the integrity and quality of the personnel involved in the warrantry process both in the agencies and the government departments concerned. I regard it as one of my functions to check these matters so far as I can and as a result I am as satisfied as I believe I possibly can be that the applications made during the year in question properly reflected the position at the time of submission, and that the Secretaries of State have properly exercised their powers under the Acts.

In his 2007 report, Lord Brown's successor as Intelligence Services Commissioner Sir Peter Gibson said:[468]

> In issuing warrants and authorisations the respective Secretaries of State must largely rely on the accuracy of the information contained in the application and the candour of those applying for it. This depends essentially upon the integrity and quality of the personnel involved in the warrantry process both in the agencies and the government departments concerned and the care with which such applications are prepared and scrutinised. Because of the legal requirements governing such warrants and authorisations increasing use is made of the legal advisers in the agencies and departments with a view to ensuring due compliance with such requirements. I regard it as one of my functions to check these matters so far as I can and as a result I am as satisfied as I believe I possibly can be that the applications made during 2007

465. Lord Brown of Eaton-under-Heywood, *Report of the Intelligence Services Commissioner for 2005-2006* (HC 314, February 2007), para 31.
466. Sir Swinton Thomas, *Report of the Interception of Communications Commissioner for 2005-2006* (HC 315, February 2007), para 14.
467. See n465 above, para 29.
468. Sir Peter Gibson, *Report of the Intelligence Services Commissioner for 2007* (HC 948, July 2008), para 31.

> properly reflected the actual circumstances at the time of submission, and that the respective Secretaries of State have properly exercised their statutory powers.

Just as we saw in Chapter 3 in relation to the making of interception warrants, however, there are good reasons to be somewhat skeptical of these cut-and-paste accounts of the Secretary of State's independence when it comes to authorising intrusive surveillance on behalf of the intelligence services.

228. As Lord Neuberger noted in the Binyam Mohamed case, in which the government challenged the Divisional Court's decision to disclose a summary of foreign intelligence contrary to the control principle, the Foreign Secretary was reliant on the advice of MI5 when preparing the public interest immunity certificates:[469]

> as the evidence showed, some Security Services officials appear to have a dubious record relating to actual involvement, and frankness about any such involvement, with the mistreatment of Mr Mohamed when he was held at the behest of US officials. I have in mind in particular witness B, but the evidence in this case suggests that it is likely that there were others. *The good faith of the Foreign Secretary is not in question, but he prepared the certificates partly, possibly largely, on the basis of information and advice provided by Security Services personnel. Regrettably, but inevitably, this must raise the question whether any statement in the certificates on an issue concerning the mistreatment of Mr Mohamed can be relied on, especially when the issue is whether contemporaneous communications to the Security Services about such mistreatment should be revealed publicly.* Not only is there some reason for distrusting such a statement, given that it is based on Security Services' advice and information, because of previous, albeit general, assurances in 2005, but also the Security Services have an interest in the suppression of such information.

The 2010 report of the Intelligence Services Commissioner made no mention, however, of the Master of the Roll's criticism of the Security Service activities in this case.

229. In her report on the 7/7 inquests, the Assistant Deputy Coroner Lady Justice Hallett similarly highlighted concerns about 'inaccurate and potentially misleading' information provided by the Security Service to the Intelligence and Security Committee during its own inquiries into the bombings:[470]

> The evidence of Witness G and the documents examined in the course of the Inquests revealed a number of inaccuracies in the ISC's otherwise detailed and thorough reports … It is unfortunate to say the least that a body established by Parliament to review the work of the Security Service, in closed hearings, reported inaccurately in these regards and that these points were not corrected … *It is essential that the ISC receives accurate information from the Security Service so that it can properly hold the Service to account,* and report to the Prime Minister, Parliament and the public … I remain concerned that in 2010, I was addressed on the basis that a statutory body had conducted, effectively, the very exercise upon which I was being asked to embark. I then discovered that the

469. *R (Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65 at para 168. Emphasis added.
470. Coroner's Inquests into the London Bombings of 7 July 2005: Report under Rule 43 of the Coroner's Rules 1984 (6 May 2011), paras 110-116. Emphasis added.

> statutory body, *the ISC, may have been inadvertently misled and thus that its reports may not have sufficiently addressed some of the central issues before it.*

Given the doubts expressed by senior judges, therefore, about the reliability and accuracy of some of the information provided by MI5 in high-profile cases, this raises the question – as in the Binyam Mohamed case – of how much faith we can have in the resulting decision of the Secretary of State, whether it is a public interest immunity certificate or a warrant to conduct intrusive surveillance. And, as we noted in Chapter 3, the political pressures on the Secretary of State make him ill-placed to the assessments of the intelligence services, especially when it comes to the necessity and proportionality of surveillance in cases involving national security.

230. The arguments raised in Chapter 3 against the role of the Secretary of State in relation to interception warrants apply with equal force, therefore, to his role authorising intrusive surveillance under Part 2 of RIPA, not to mention warrants for the interference with property under Part 3 of the Police Act 1997.

Lack of comprehensive oversight

231. The current regime for oversight of authorisations for intrusive surveillance under Part 2 of RIPA and Part 3 of the Police Act is plainly unsatisfactory for a number of reasons.

232. First, the current distinction between 'property interference' and 'intrusive surveillance' does not arise from any discernable logic but from mere accident of history. The very language of property interferences and wireless telegraphy was an artifact of the Security Service Act 1989, rushed through Parliament to anticipate the ruling in *Harman and Hewitt,* and designed around what was then the primary means of conducting audio surveillance. This, in turn, became the model that was adopted by Parliament when it rushed through the Police Act in 1997 to anticipate yet another adverse judgment of the Strasbourg Court following *R v Khan*.

233. By February 2000, however, when RIPA was first introduced in Parliament, supervening changes in both communications and surveillance technology since the original 1989 Act had considerably reduced the need to interfere with property and made statutory references to 'wireless telegraphy' in the context of surveillance virtually antique.[471] Rather than take the opportunity afforded by RIPA to start afresh with a more coherent and principled framework, though, the government opted instead to lash its new provisions for intrusive surveillance onto the pre-existing frameworks of the Intelligence Services Act 1994 and the Police Act 1997. This gives rise to what is effectively a four-way split involving two different oversight commissioners and three different Acts, c.f.:

(a) intrusive surveillance by the police under Part 2 of RIPA is overseen by the Chief Surveillance Commissioner;

(b) intrusive surveillance by the intelligence services under Part 2 of RIPA is overseen by the Intelligence Services Commissioner;

471. See section 116(2) of the Wireless Telegraphy Act 2006 for the most up-to-date definition.

(c) warrants for property interference by the police under Part 3 of the Police Act 1997 are overseen by the Chief Surveillance Commissioner; and

(d) warrants for property interference by the intelligence services under the Intelligence Services Act 1994 are overseen by the Intelligence Services Commissioner.

It seems difficult to conceive of a more arbitrary and piecemeal way for regulating what is essentially the same activity in each case.

234. Second, these highly-fragmented oversight arrangements make it more difficult for members of the public to form an accurate picture of how powers of intrusive surveillance and property interference are being exercised by the police, the intelligence services and other agencies. This, in turn, limits their ability to effectively debate, among other things, whether the law strikes the correct balance between the interests of law enforcement and national security, on the one hand, and the protection of the right to privacy, on the other.

235. Third, this difficulty in securing effective public oversight of the use of intrusive surveillance is compounded by markedly different levels of transparency provided by the different oversight commissioners under RIPA. As noted in earlier chapters, there are of course some inevitable difficulties in providing effective transparency in respect of secret surveillance. For a start, there is the obvious need to maintain operational secrecy concerning any investigation that may be ongoing. There is also the need to ensure that details about the particular methods or techniques that may be used by investigators are not unduly disclosed. This is particularly true concerning the work of the intelligence services who work mostly in secret. This, however, is not enough to explain the general disparity between the generally good level of transparency provided by the Office of the Surveillance Commissioners, on the one hand, and the generally woeful level of transparency provided by the Intelligence Services Commissioner on the other.

236. The Office of the Surveillance Commissioner, for instance, has a both a website[472] and an email address for the public.[473] The former contains not only the annual reports of the Chief Surveillance Commissioner but also relevant primary and secondary legislation, a selection of case law, Codes of Practice as well as guidance for officials using RIPA. The Chief Surveillance Commissioner, moreover, has continued to press for more resources to upgrade the website.[474] In particular, the annual reports give detailed statistics on authorisations, including a breakdown of the numbers in relation to particular types of offences (although, as noted above, more information could yet be provided, eg, the number of applications for intrusive surveillance that are refused by the Commissioners each year). Although we are concerned at the apparently low number of authorisations quashed by the Surveillance Commissioners, the fact that there are any at all stands in marked contrast to most other parts of RIPA.

472. www.surveillancecommissioners.independent.gov.uk
473. www.surveillancecommissioners.independent.gov.uk/contact.html
474. See Rose, *Annual Report of the Chief Surveillance Commissioner 2008-2009* (HC 704, July 2009), para 3.21: 'I rely on the resources of others to maintain this website. I do not have the capacity to improve the website in the way that I had hoped but improvement remains an aspiration'; see also his annual report for 2009-2010 (HC 168, July 2010), para 3.15: 'I have not had the capacity to improve the website as I had hoped; it is in need of an upgrade'; and his annual report for 2010-2011 (HC 1111, June 2011): 'I have not had the capacity to improve my website. The Cabinet Office has recently decided that all government related websites, including those of Non Departmental Public Bodies such as mine, will migrate to a corporate process. It is essential that I remain independent and be seen to be independent'.

237. The Intelligence Service Commissioner, by contrast, has no website, no email address, and no other apparent contact details apart from a postal address, 'c/o 2 Marsham Street', ie, the Home Office. Although his work is mentioned on the website of the IPT,[475] the only official website to carry his annual reports appears to be MI5.[476] As with the reports of the Interception Commissioner discussed in Chapter 3 and as we have already seen in the previous section, the annual reports of the Intelligence Services Commissioner have for most of the last decade disclosed little and appeared to rely heavily on the same language being reused year after year.

238. And as with the Interception Commissioner, the Intelligence Services Commissioner appears never to have reviewed a warrant or authorisation under Part 2 of RIPA or under section 5 of the Intelligence Services Act 1994 in which he judged the Secretary of State's decision to be either unnecessary or disproportionate under Article 8(2). And, as with the Interception Commissioner, we do not even know the proportion of warrants and authorisations that are reviewed by the Intelligence Services Commissioner. In his 2001 report, for instance, Lord Brown said:[477]

> I have read the files relating to *many* of the warrants and authorisations issued during the course of the year and some of those where the warrants previously issued have been renewed.

By the time of his annual report for 2003, however, 'many' had been downgraded to 'a number':[478]

> I have read the files relating to a *number* of warrants and authorisations issued during the course of the year and some of those where the warrants or authorisations previously issued have been renewed.

239. Indeed, if such a thing were possible, the reports of the Intelligence Services Commissioner manage to disclose even less information than those of the Interception Commissioner. The latter, at least, gives annual figures for the number of interception warrants issued by the Home Secretary and the Scottish Executive. By contrast, the number of warrants and authorisations made by the Secretary of State on behalf of the intelligence services under either Part 2 of RIPA or the 1994 Act remains completely unknown. In his most recent report, Sir Peter Gibson explained his adherence to this long-standing practice:[479]

> I will not disclose publicly the numbers of warrants or authorisations issued to the security and intelligence agencies or the armed forces. That is because it would, I believe, assist those unfriendly to the UK were they able to know the extent of the work of the Security Service, SIS, GCHQ and the armed forces in fulfilling their functions.

475. www.ipt-uk.com/default.asp?sectionID=8&chapter=1
476. www.mi5.gov.uk/output/intelligence-services-commissioner.html
477. *Report of the Intelligence Services Commissioner for 2001* (HC 1244, October 2002), para 28.
478. *Report of the Intelligence Services Commissioner for 2003* (HC 884, July 2004), para 28.
479. Gibson, *Report of the Intelligence Services Commissioner for 2010* (HC 1240, June 2011), para 46. See eg, Lord Brown, 2001 report, n477 above, para 30: 'In his previous reports as Intelligence Services Commissioner and Security Service Commissioner my predecessor explained the reasons for not disclosing the numbers of warrants or authorisations issued to the agencies. I agree with his view that particulars of the actual numbers would assist the operation of those hostile to the state if they were able to estimate even approximately the extent of the work of the Security Service, SIS and GCHQ in fulfilling their functions'.

As with the number of interception warrants issued by the Foreign Secretary or the Northern Ireland Secretary, however, the claim that publishing the number of warrants or authorisations under RIPA or the 1994 Act would assist those hostile to our national interests seems difficult to justify. Certainly, it is hard to see how, in comparable circumstances, the national security of the United States is undermined by the fact that the Department of Justice reports annually to Congress the precise number of warrants and authorisations under the Foreign Intelligence Surveillance Act. Even if it were true that publishing the numbers were to assist the work of terrorists and foreign saboteurs, any advantage they gained as a result must surely be a slender one, and is surely outweighed by the net benefits to democratic transparency. After all, if the national security of the United States can survive publication of the numbers, the UK can surely weather the storm.

Flawed definition of 'intrusive'

240. In principle, at least, the definition of 'intrusive' under Part 2 of RIPA is supposed to be a significant safeguard against unnecessary or disproportionate interference with the right to privacy under Article 8. The requirement for prior judicial approval of any authorisation of intrusive surveillance – for police and other law enforcement agencies at least – is meant to ensure that any surveillance activities that are likely to involve serious interference with a person's privacy, whether it is direct or collateral, are subject to a much higher degree of scrutiny than authorisations for directed surveillance (see Chapter 6).

241. As we have already seen in relation to legal professional privilege, however, it is clear that the definition of 'intrusive' under Part 2 fails to properly capture the full range of surveillance activities that could reasonably be expected to involve serious interference with privacy. As the Code of Practice itself notes:[480]

> The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained … Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of *private information*.

Even under the terms of the 2010 Order, there is no requirement to obtain authorisation for intrusive surveillance if, for example, the police reasonably believe that a suspect and his lawyer are having privileged conversations in an apparently isolated section of a public park, and they attempt to use a long-range directional microphone to listen in. By way of contrast, Part 3 of the 1997 Act requires authorisations for property interference to be subject to prior judicial approval *wherever* they are likely to result in the 'acquisition of knowledge of matters subject to *legal privilege*, confidential personal information or confidential journalistic information'.[481]

242. Even as supplemented by the 2010 Order, therefore, the definition of 'intrusive surveillance' under Part 2 gives rise to a clear risk that surveillance decisions that are likely to involve serious interference with privacy under Article 8(2) will not be subject to adequate and effective safeguards against abuse: specifically, that the assessment of whether it is necessary and proportionate to interfere with someone's privacy in this way will not be subject to the prior judicial approval of a

480. Para 2.11. Emphasis in original.
481. Ibid, para 4.12. Emphasis in original.

Surveillance Commissioner. As Lord Neuberger noted, concerning the Secretary of State's delay in implementing the Divisional Court's ruling in *In re C* in December 2007:[482]

> Having decided not to appeal the Divisional Court's decision that surveillance of privileged and private consultations under the present regime is unlawful, the Secretary of State should have ensured that such surveillance did not take place or she should have promptly changed the regime so as to comply with the Divisional Court's decision. As Lord Carswell points out, more than a year has elapsed since that decision, and your Lordships were told that the Secretary of State was not even in a position to produce a draft regulation embodying the changes to ensure that such surveillance was carried out legally. *Unless no surveillance of privileged and private consultations has been going on for the past year in the United Kingdom (which appears most unlikely), this strongly suggests that the Government has been knowingly sanctioning illegal surveillance for more than a year.* If that is indeed so, to describe such a state of affairs as 'regrettable' strikes me as an understatement.

Lord Neuberger's judgment was handed down in March 2009. However, the Order requiring surveillance of privileged communications in custody to be treated as intrusive was not made until 25 February 2010. In other words, the government appears to have been knowingly sanctioning illegal surveillance of privileged communications for more than two years.

Recommendations

Establish a single warrant for intrusive surveillance and property interference

243. The existing distinction between authorisations for property interference and/or wireless telegraphy under the 1994 and 1997 Acts and intrusive surveillance under Part 2 of RIPA is not only obscure and analytically unperspicacious, but also fails to reflect more than 20 years worth of changes in surveillance and communications technology. Although it is true that not all interference with property necessarily involves intrusive surveillance, it is always ancillary to surveillance in one way or another. No useful purpose is served, moreover, by maintaining a distinct legal regime to address it spread across two different Acts.

244. We, therefore, recommend that provisions for property interference should be assimilated into a new single-warrant structure for intrusive surveillance and property interference (renamed simply 'surveillance warrants'). This would include broadening the definition of 'intrusive' to cover *all* surveillance likely to constitute a serious interference with a person's privacy under Article 8, eg, *any* surveillance of privileged communications, confidential personal information or confidential journalistic information. At the same time, it would also be appropriate to limit the definition of property interference to exclude, for instance, incidental interference with public property.

482. *In re McE,* n382 above, para 119. Emphasis added. See also Rose, 2007-2008 report, (HC 659, July 2008), para 3.4: 'The Commissioners have deduced that they do not currently have the statutory powers to provide the independent judicial oversight required by the judgment delivered in the High Court of Justice in Northern Ireland, Queen's Bench Division (Judicial Review) in the matter of an application by C, A, W, M and McE ([2007] NIQB 101) relating to the conduct of covert activity that is considered likely to acquire confidential information as defined by the legislation'.

All surveillance warrants to be made by a judge

245. The role of the Secretary of State in authorising intrusive surveillance under Part 2 of RIPA and property interference under Part 3 of the Police Act 1997 should be removed and replaced by a regime of surveillance warrants issued by a Surveillance Commissioner, regardless of whether the surveillance is carried out by police, another law enforcement agency or the intelligence services. This would not extend, however, to the activities of the intelligence services or HM forces overseas.

246. We also recommend that the process currently provided by Part 2 of RIPA of executive authorisation followed by judicial approval should be replaced with the much more straightforward process of allowing agencies to apply directly to the Surveillance Commissioners (or, alternatively, Crown Court judges) for surveillance warrants (see below). Existing arrangements for self-authorisation by a senior member of the agency in cases of emergency should be retained, to be followed by judicial confirmation within 48 hours.

Streamline existing oversight arrangements

247. In line with our previous recommendations, we consider it desirable that the same essential activity (ie, the granting of surveillance warrants) should be subject to a single oversight regime. The limited oversight provided by the Intelligence Services Commissioner in respect of Part 2 and warrants under the 1994 Act is deeply unsatisfactory, whereas that provided by the Chief Surveillance Commissioner in respect of Part 2 and the 1997 Act appears to work well. We, therefore, recommend that responsibility for oversight should similarly pass to the Chief Surveillance Commissioner. It may be that there is a continuing role for the Intelligence Services Commissioner, however, in respect of the overseas activities of the intelligence services, although this may be something better addressed in relation to discussions about broader reform of the Security and Intelligence Committee.

Chapter 6
'Directed' surveillance

248. Like the concept of 'intrusive' surveillance discussed in Chapter 5 and unlike the more well-established surveillance powers such as the interception of communications under Part 1 or interference with property under the Police and Intelligence Services Acts, the concept of 'directed' surveillance was one that was invented specifically for the purposes of Part 2 of RIPA.

249. Unlike intrusive surveillance, however, the power to conduct directed surveillance is not restricted to law enforcement or intelligence agencies, but – like the power to access communications data – is a power enjoyed by a very large number of public bodies. There are at least two reasons for this: the first is that, as we shall see shortly, the definition of directed surveillance is much broader than that of intrusive surveillance and so applies to the investigative activities of a much wider range of bodies, eg, the use of ANPR cameras in the local council car park; the second is that because – by definition – directed surveillance is not as intrusive, and not restricted to the investigation of serious crime, it was thought by the government to be equally appropriate to the activities of non-law enforcement bodies, eg, the Food Standards Agency, Royal Pharmaceutical Society of Great Britain.

250. In addition to the general definition of surveillance under Part 2 of RIPA (set out in Chapter 5), 'directed' surveillance is defined as surveillance which is:[483]

    a) covert;[484]

    b) not intrusive;

    c) for the purposes of a specific investigation or operation;

    d) likely to result in private information being obtained about any person; and

    e) not an immediate response to circumstances in which it wouldn't be reasonably practicable for an authorisation to be sought.

'Private information' is further defined as including any information relating to a person's private or family life.[485] The Code of Practice goes on to advise that:[486]

483. Section 26(2).
484. Section 26(9)(a) and see also Chapter 5 above.
485. Section 26(10).
486. Code of Practice, para 2.6. Emphasis in original.

> Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute *private information* even if individual records do not.

251. Authorisations for directed surveillance may be made by the designated person within each public body, as prescribed by regulations. Sections 28(2) and (3) provide that he shall not do so unless he believes that it is necessary and proportionate in the interests of national security; preventing or detecting crime; preventing disorder; for the economic well-being of the UK; for public safety; protecting public health; assessing or collecting any tax or duty, etc.; or for any other purpose that the Secretary of State may designate. As with authorisations for intrusive surveillance, authorisations for directed surveillance make it 'lawful for all purposes'. In other words, it does not make *un*authorised surveillance illegal, but it does immunise authorised surveillance from civil liability.

252. The use of directed surveillance by public bodies is subject to the oversight of the Chief Surveillance Commissioner, with the exception of directed surveillance carried out by the intelligence services which is overseen by the Intelligence Services Commissioner. In addition, the IPT has jurisdiction to hear complaints concerning the use of directed surveillance.

253. Between April 2002 and March 2011, there have been 186,133 law enforcement authorisations for directed surveillance by law enforcement bodies. Between April 2003 and March 2011, there have been 68,317 authorisations for directed surveillance by non-law enforcement bodies (including government departments and local authorities). The majority of authorisations for directed surveillance by non-law enforcement bodies is by government departments rather than local authorities. The number of authorisations for directed surveillance made by the intelligence services is not known.

Flawed definition of 'directed'

254. As we saw in Chapter 5, the definition of 'intrusive' in Part 2 of RIPA is seriously flawed, such that many kinds of surveillance which are likely to result in a serious interference with a person's privacy are not covered by the definition. The flipside of this is that the definition of 'directed' surveillance is equally flawed, for it, by definition, includes those kinds of surveillance which are covert but not intrusive. This means that, in many cases, public authorities are effectively able to self-authorise intrusive surveillance of individuals without having to obtain the approval of a Surveillance Commissioner and with minimal ex post facto oversight from the Chief Commissioner's office.

255. As mentioned already in previous Chapters, the best-known instance of this has been the use of directed surveillance authorisations to conduct covert surveillance of conversations between lawyers and suspects in police stations and prison cells by way of covert listening devices. In December 2007, the Northern Irish Divisional Court held that this breached Article 8 ECHR because directed surveillance did not involve prior judicial approval. Although the Secretary of State chose not to appeal this part of its ruling, the House of Lords affirmed it in its judgment in early 2009.[487]

487. See also eg, Rose, 2008-2009 report (HC 704, July 2009), para 3.2: 'Following publication of the opinions of the Lords of Appeal, referred to earlier in this report, it became apparent that it would be necessary to change the law to enable me to act on the suggestion that my Commissioners should provide prior approval in relevant cases. I await the enactment of the legislation'.

However, it was not until February 2010 that a Home Office minister made an order directing that surveillance of privileged communications in custody, places of detention, court buildings and lawyers' offices was to be authorised as 'intrusive' rather than 'directed' surveillance. Even the 2010 order, however, left open the loophole of using directed surveillance to monitor privileged communications in other settings, eg, a town hall or an MPs office.

256. More generally, the ever-increasing power and sophistication of surveillance devices has meant that it is possible to gather more and more private information about individuals without the need to intrude on their residences, making the definition of 'directed' surveillance even less adequate. In *Uzun*, for instance, the ECtHR distinguished between less intrusive methods of surveillance, such as GPS tracking of a suspect's car, and more intrusive methods such as interception or 'other methods of visual or acoustical surveillance', because the latter tended to 'disclose more information on a person's conduct, opinions or feelings'.[488] But the increasingly pervasive nature of digital surveillance means that even apparently less-intrusive methods may yet gather considerable information about a person's 'conduct, opinions or feelings'.[489] Similarly, as the ECtHR noted in *Peck*, although 'the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data' does not normally give rise to an interference with that person's private life, the *recording* of such data 'and the systematic or permanent nature of the record may give rise to such considerations'.[490]

257. Section 26(5) of RIPA requires that surveillance of residences and vehicles carried out by way of an external surveillance device (eg, a directional microphone across the street from someone's house) will count as 'intrusive' surveillance if it 'consistently' provides 'information of the same quality and detail' that would be expected of an internal device. In his evidence to the House of Lords Constitution Committee in 2008, the Chief Surveillance Commissioner gave an example of how this statutory definition was under constant pressure from technological developments:[491]

> I think the problem arises from the statutory definition of what is intrusive. What is intrusive for this purpose is if you have a device which is capable of providing you with information of the quality which you would get if you were yourself in the motor car or in the house. ANPR highlights this particular problem, because in 2000, when the legislation was passed, the technique was adequate for recognising number plates. The technique is now capable of identifying not only the number plate, not only the driver, not only the front seat passenger, but the back seat passengers as well.

258. But the definition of directed surveillance in general makes no allowance for other kinds of surveillance that, while not carried out in relation to a residence or vehicle (and hence is not intrusive under section 26(3)), is nonetheless likely to result in privileged, confidential or otherwise highly personal information about a person being obtained. For example, an operation involving a covert camera situated across the street from a building known to host weekly meetings of Narcotics Anonymous, for the purpose of determining whether and how often a particular person attends those meetings, would not count as intrusive because the building is not used as a residence, and the camera is only used to monitor the entrance not the building's interior.

---

488. See n174 above.
489. See eg, Royal Academy of Engineering, *Dilemmas of Privacy: Challenges of Technological Change* (March 2007).
490. See n133 above, para 59.
491. Evidence of the Chief Surveillance Commissioner to the House of Lords Constitution Committee, 21 May 2008, Q673.

259. As we will see below, however, the inadequate procedures for authorisation and subsequent oversight of directed surveillance mean that it is extremely unlikely that a wrongful decision will be detected, particularly where the public body in question elects not to use the material obtained as evidence in subsequent proceedings. Part 2 of RIPA, therefore, fails to offer adequate or effective safeguards against unnecessary or disproportionate use of both intrusive and directed surveillance.

Inadequate authorisation

260. As we have already seen in Chapter 4, any kind of surveillance power which fails to be authorised by a senior member of the public body carrying out the interception involves certain inherent risks, not the least of which is that the official will merely rubber stamp the application of his or her subordinates rather than carry out the assessment. It's necessity and proportionality that section 28 requires. We do not suggest that senior officials do not provide any kind of safeguard whatsoever: no doubt some senior officials discharge their responsibilities with great diligence. They are also subject to the oversight of the Chief Surveillance Commissioner, which includes an inspection regime that is meant to ensure that each public body able to exercise surveillance powers has the necessary training and internal procedures to comply with the requirements of Part 2.

261. But, as we have noted in previous chapters, it is generally unrealistic to expect senior members of public bodies which have a vested interest in the prevention and detection of crime, etc., to objectively assess the merits of particular surveillance decisions that would likely enable them to better carry out their functions. This is particularly the case where the public body in question is under pressure from government ministers or the public to achieve targets or results, as many public bodies are. As the Chief Surveillance Commissioner Sir Christopher Rose noted in 2008: 'the setting of performance targets can adversely influence the judgement of necessity and proportionality'.[492] In his most recent report in 2011, he also noted for instance that:[493]

> My inspections have revealed pressure on some authorising officers to grant covert surveillance to meet Government targets for incognito inspections (commonly termed 'test purchases').

262. The annual reports of the Chief Surveillance Commissioner otherwise generally attest to a reasonable level of compliance by public bodies with the requirements of Part 2.[494] As Sir Christopher Rose wrote in his most recent report, for instance, 'local authorities are, generally speaking, exercising their powers properly'.[495] At the same time, however, his reports also make reference to significant problems with the authorisation procedures of a number of public bodies. In 2005, for instance, he noted that 'many public authorities are vulnerable to challenge because the concept of 'proportionality' is still not properly understood'.[496] The following year he wrote:[497]

492. Rose, 2007-2008 report (HC 659, July 2008), para 8.14
493. Rose, 2010-2011 report (HC 1111, June 2011), para 5.6.
494. See eg, Rose, ibid, paras 5.2-5.3: 'I am broadly satisfied, from the inspections that my organisation is able to conduct, that public authorities are generally acting in a manner compliant with the legislation'.
495. Ibid, para 5.4. Indeed, as the reports show, the great majority of authorisations for directed surveillance are made by the police and other law enforcement agencies. Authorisations by other public bodies make up on average about 38% of the total each year, and the majority of these are by government departments rather than local authorities.
496. 2004-2005 report (HC 444, November 2005), para 10.7. Emphasis added.
497. 2005-2006 report (HC 1298, July 2006), para 8.11. Emphasis added.

> During the year authorisations for directed surveillance have failed to achieve the improvements which were needed. *In many instances applications continue to confuse necessity, proportionality and collateral intrusion*. Inexperienced authorising officers compound the problem by providing unintelligent authorisations that sometimes do not authorise the particular activity applied for. *This leads to unauthorised covert activity,* and may render any product obtained inadmissible in criminal proceedings

In 2007, he similarly noted that 'there remains a generally poor understanding of the concept of proportionality, particularly by applicants',[498] and in 2008 he said:[499]

> The evidence is that [some] local authorities tend to resort to covert activity as a last resort but, when they do, have a tendency to expose lack of understanding of the legislation by completing documentation poorly. *In particular there is a serious misunderstanding of the concept of proportionality.* It is not acceptable, for example, to judge, that because directed surveillance is being conducted from a public place, this automatically renders the activity overt or to assert that an activity is proportionate because it is the only way to further an investigation.

And in 2011 he reported that his inspections of public authorities revealed:[500]

> *a tendency to confuse the role of the applicant and the role of the authorising officer.* The former is required to provide the intelligence underpinning the investigation, to outline the plan of action and to request specific methods and equipment. The latter is the person who decides whether the application meets the tests of necessity and proportionality and considers whether sufficient attention has been paid to minimising collateral intrusion. *Too often applicants (or other gatekeepers in the case of law enforcement agencies) are presenting applications which assert that the activity is necessary and proportionate. Some authorising officers then simply repeat or endorse the application instead of applying their minds to the relevant criteria in the circumstances of the specific case.*

This practice of authorising officers simply repeating or endorsing the application is, of course, better known as 'rubber stamping'. The details that emerge from Sir Christopher's reports are, in this way, frequently at odds with his more general conclusions. It is, nonetheless, to his credit that these problems are at least identified in his reports. There is, by contrast, next to nothing in any of the annual reports of the Intelligence Services Commissioner to suggest the slightest problem with the intelligence service's use of directed surveillance.

263. Ongoing public concern about the proportionality of the use of surveillance powers by local authorities in particular was brought to a head in 2008 when it emerged that Poole Borough Council had authorised directed surveillance of a family of five, in order to investigate whether the parents had lied about their primary residence on an application form in order to send one of their children to the local school.

---

498. 2006-2007 report (HC 713, July 2007), para 8.6.
499. 2007-2008 report (HC 659, July 2008), paras 9.2-9.3. Emphasis added.
500. 2010-2011 report, para 5.8; see also 2007-2008 report, para 9.3: 'The inexperience of some authorising officers is matched, in many cases, by poor oversight by those nominated as monitoring officers and a tendency for Chief Executives not to understand the risks that face their authorities'; see also ibid, para 9.7: 'Another common weakness is where the authorising officer is head of the department conducting the surveillance. If an authorising officer is too close to the investigation it is difficult to demonstrate the independence and objectivity encouraged by the legislation'.

264. The authorisation was granted by the council's head of legal services and included permission to observe 'the day to day movements of the family' by 'use of a digital camera to record images of persons entering and/or exiting both addresses'.[501] The surveillance lasted three weeks and involved the Council education officer driving past two properties owned by the family to see whether they were being used, parking nearby in order to watch who was getting in or out of the family car, and on one occasion following the mother on a school run.[502]

265. Despite a widespread public outcry, the Chief Surveillance Commissioner declared that 'media criticism of Poole Borough Council was misplaced'.[503] The Home Office nonetheless consulted on whether to remove surveillance powers, including the use of directed surveillance from a number of public bodies. As it was, however, only one – the Ministry of Defence – lost the power entirely.[504] And in July 2010, the IPT ruled that Poole's authorisation to carry out surveillance of the family had been unnecessary and disproportionate, and thus contrary to Article 8 ECHR.[505] However, the Tribunal refused to rule out that using surveillance operations for the sake of investigating possibly dishonest applications for school places was generally outside the scope of RIPA.[506]

266. The Coalition government's promise in April 2010 to restrict the power of local authorities to use surveillance powers and the conclusions of the Home Office review of Counter-Terrorism Powers has already been referred to in Chapter 4. In relation to the use of directed surveillance, the review recommended not only that 'magistrate's approval should be required' but also:[507]

> Use of RIPA to authorise directed surveillance only should be confined to cases *where the offence under investigation carries a maximum custodial sentence of 6 months or more.* But because of the importance of directed surveillance in corroborating investigations into underage sales of alcohol and tobacco, the Government should not seek to apply the threshold in these cases. The threshold should not be applied to the two other techniques [communications data and covert human intelligence sources] because of their more limited use and importance in specific types of investigation which do not attract a custodial sentence.

267. As with its provisions on communications data, clause 38 of the Protection of Freedoms Bill would require any local authority authorisation for directed surveillance or the use of a covert human intelligence source to obtain prior judicial approval before taking effect. And it would also allow the Secretary of State to extend by order the same requirement to other public bodies under Part 2 of RIPA. In his evidence to the Public Bill Committee and in his most recent report, however, the Chief Surveillance Commissioner criticised the Bill's proposals:[508]

> *Leaving aside the cost of training and reimbursing many more magistrates than there are authorising officers, it is not apparent why local authorities should be treated differently from other public authorities* and, as is apparent from this and my previous Annual Reports, local authorities are, generally speaking, exercising their powers properly.

501. *Paton v Poole Borough Council* (IPT/09/01/C, 29 July 2010), paras 14 and 21.
502. Ibid, paras 43-44.
503. 'The Oversight Role of the Chief Surveillance Commissioner', speech to the Commonwealth Club, 10 February 2009, p5.
504. The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).
505. Ibid, paras 60-73.
506. Ibid, para 65.
507. N349 above, p27. Emphasis added.
508. Rose, 2010-2011 report (HC 1111, June 2011), para 5.4. Emphasis added.

In particular, Sir Christopher noted that, since Part 2 does not make unauthorised surveillance necessarily unlawful, the requirement of prior judicial approval would not, in fact, lead to more proportionate use of surveillance but more *unauthorised* surveillance: [509]

> The higher threshold [of six months] in the proposed legislation will reduce the number of cases in which local authorities have the protection of RIPA when conducting covert surveillance; *it will not prevent the use of those tactics in cases where the threshold is not reached but where it may be necessary and proportionate to obtain evidence covertly and there will be no RIPA audit trail.*

If, however, a local authority has no lawful authority to use covert surveillance in order to investigate a crime for which the maximum penalty is less than six months imprisonment then, contrary to Sir Christopher's claim, it can never be either 'necessary or proportionate' for it to use unauthorised surveillance in such a case. This is because the question of whether an interference with someone's privacy is necessary or proportionate under Article 8(2) is incapable of arising unless that interference is also 'in accordance with the law'. This would, in turn, amount to a breach of the public body's duty to act compatibly with Convention rights under section 6 of the Human Rights Act. The suggestion that restricting the lawful use of surveillance powers by public bodies might encourage those public bodies to act unlawfully is, therefore, difficult to take seriously as a criticism of the Bill's proposals.

268. More generally, Sir Christopher's claim that local authorities are generally 'exercising their powers properly' means only that they are, by and large, acting within the principles laid down by Part 2 of RIPA. This is nothing to the larger point, however, that Part 2 of RIPA is itself too broad because it enables surveillance to be used for the sake of investigating relatively minor crimes. As the Strasbourg Court held in its recent judgment in *Uzun*, the seriousness of the offending is a major factor in determining whether the interference with privacy caused by covert surveillance will be proportionate.[510]

269. Conversely, it could be said that Part 2 was adequate so long as the government exercised restraint in only including those public bodies with responsibility to investigate serious wrongdoing. It is a reasonable criticism of the Coalition government's proposals in the Protection of Freedoms Bill that they are targeted first and foremost on local authorities, when – as Sir Christopher points out – many other non-law enforcement bodies also have the power to use directed surveillance, eg, the Charity Commission or the Department for Business Innovation and Skills. Certainly, there was nothing in RIPA as it was originally enacted to require that so many public bodies should be given the power to carry out directed surveillance. But just as a public body's right to access data creates its own demand for that data, as the Newton Committee of Privy Councillors noted in 2003, so too does the grant of surveillance powers to a wide range of bodies generate a similar demand for their use, as the sorry case of Poole Borough Council plainly shows.[511]

509. Ibid, para 5.4. Emphasis added.
510. N174 above, para 80. Emphasis added.
511. See eg, Rose, 2010-2011 report, para 5.11: 'We have evidence that some public authorities are purchasing highly intrusive technical capability without properly considering the legislative implications of its use'; see also eg, 2006-2007 report, para 11.2: 'I have been informed that some authorities have made enquiries with their local police force regarding the acquisition of tracking technology. This is clearly a capability that local authorities are not entitled to use because it would entail property interference and, in some cases, may result in intrusive surveillance'.

Inadequate oversight

270. The wholesale absence of prior judicial authorisation for directed surveillance under Part 2 makes the mechanisms for ex post facto review all the more important as a check against abuse. As the ECtHR said in *Uzun* concerning less intrusive types of surveillance, lack of sufficient independence at the initial authorising stage can be offset to a certain extent by subsequent judicial review. In particular, it said, the possibility that evidence gained from the surveillance might be excluded by a judge at trial was 'an important safeguard' against arbitrary interference with Article 8, 'as it discouraged the investigating authorities from collecting evidence by unlawful means'.[512] As the Chief Surveillance Commissioner has noted, however, 'only a small proportion of covert activity results in material which is tendered in evidence in court'.[513] Nor is it an effective sanction in cases where the purpose of the surveillance is intelligence-gathering (including criminal intelligence) rather than the gathering of evidence.

271. Authorisations under Part 2 are also subject to the oversight of the Chief Surveillance Commissioner, which includes an inspection regime for all public bodies able to carry out directed surveillance (save for the armed forces overseas and the intelligence services, whose use of directed surveillance is overseen by the Intelligence Service Commissioner).

272. In his annual reports, however, the Chief Surveillance Commissioner has stressed the limits of the check provided by his inspection regime, which covers authorisations for intrusive surveillance, directed surveillance, property interference and the use of covert human intelligence sources. In his 2010 report, for instance, Sir Christopher made clear that the proportion of authorisations that he and his inspectors are able to review for each public body depends on the volume of surveillance that it undertakes so that, for example, 'in larger law enforcement agencies I am only able to conduct a dip sample of authorisations', whereas non-law enforcement bodies tend to have a higher proportion of their authorisations examined on inspection because they 'engage in considerably less covert activity'.[514] When asked by the House of Lords Constitution Committee in 2008 whether this dip sampling approach was adequate, Sir Christopher answered:[515]

> I cannot prove that it is adequate, because the 10 per cent of documentation, or whatever it is in the particular case, which is examined may or may not be representative, so I cannot prove that it is adequate.

273. His warning concerning the limitations of his inspection regime in his 2009 annual report was even more stark:[516]

> It is important that everyone, particularly trial judges because they are the arbiters of admissibility, should appreciate that *not every authorisation presented in court has been subject to scrutiny* by the [Office of the Chief Surveillance Commissioner]. A Surveillance Commissioner sees all authorisations for property interference and

512. N174 above, para 72.
513. 2010-2011 report, para 3.5.
514. 2009-2010 report, para 3.10. Emphasis added.
515. Evidence of Sir Christopher Rose to the House of Lords Constitution Committee, 21 May 2008, Q654.
516. 2008-2009 report, para 5.12. Emphasis added. See also eg, 2010-2011 report, paras 3.10-3.12: 'I have commented in previous reports that there appears to be an over-reliance on the capacity of the OSC to examine authorisations. I remain concerned that my limited capacity is misappreciated. Public authorities, particularly law enforcement agencies, should not be lulled into a false sense of confidence if at trial lawyers do not scrutinise relevant documents. Lack of challenge does not imply compliant authorisation'.

> intrusive surveillance contemporaneously. *No authorisations for directed surveillance or the use of a CHIS are seen contemporaneously; a proportion, selected by dip sample, are seen during OSC inspections.*

In his most recent report, Sir Christopher noted the pressure imposed by limited resources, stating that the 'task of completing inspections with a frequency conducive to effective oversight is increasingly difficult'.[517] Moreover, he highlighted the fact that he has 'still not been given the power to inspect local authorities in Northern Ireland', of which there are 26 that have apparently 'never been inspected'.[518] Nor does the Chief Surveillance Commissioner appear to have oversight in relation to the use of directed surveillance in private prisons.[519]

274. The reports of the Intelligence Services Commissioner, by contrast, provide very few details of the corresponding inspection regime for the use of directed surveillance by the intelligence services. In contrast to the public testimony of the Chief Surveillance Commissioner, we have no real indication of the proportion of authorisations reviewed by the Intelligence Services Commissioner. It is difficult to see why this should not be stated openly. If any problems with intelligence services authorisations have been encountered, moreover, they have never been highlighted by the Commissioner. Unlike most other public bodies, the intelligence services do not, as a general rule, use directed surveillance to gather admissible evidence for use in criminal cases (although they may sometimes support the activities of the police, in certain circumstances). The possibility that such evidence might be excluded subsequently by a judge at trial is not, therefore, any kind of safeguard against their unnecessary or disproportionate use of either intrusive or directed surveillance.

275. In addition to these limitations, there is nothing in either Part 2 of RIPA or the Code of Practice governing intrusive and directed surveillance that requires either the Chief Surveillance Commissioner or the Intelligence Services Commissioner to notify a person in the event that they discover an authorisation that fails to comply with the statutory requirements, particularly those of necessity and proportionality.[520] As the House of Lords Constitution Committee noted in its 2009 report, moreover, Part 2 'does not provide any scope for targeted inspections in response to alleged abuses that may have caused public concern'.[521] When the Committee asked Sir Christopher if he would consider investigating specific cases, he answered:[522]

> Certainly not. It would be totally impossible to do that. As I say, there are a very large number of authorities which we inspect, we have a carefully designed programme. I mean, I am not ruling it out absolutely, if there was a well documented manifest abuse of power by a local authority, well then, of course we would try and do something about it, but I am afraid responding to press reports is not always a fruitful activity when you only have a small amount of resources at your disposal.

---

517. 2010-2011 report, para 3.7. See also eg, 2010-2011 report, para 3.25: My capacity has always been limited and I wrote to the Home Secretary to explain the impact of reducing my budget by £140K. I recognise the severity of the country s financial situation but a reduction of nine percent has serious operational repercussions in a tiny organisation. I am only able to work within this tight limit by reducing inspectorate and secretarial staff ; see also, 2010-2011 report, para 6.5: I am concerned that my reduced budget may have an adverse impact on my ability to fulfil properly my statutory oversight responsibility .
518. 2010-2011 report, para 3.12.
519. 2006-2007 report, para 8.12.
520. Home Office, *Covert Surveillance and Property Interference: Revised Code of Practice* (2010).
521. N72 above, para 256.
522. Evidence of the Chief Surveillance Commissioner to the House of Lords Constitution Committee, 21 May 2008, Q653. See also eg, 2008-2009 report, para 3.7: 'I consider it necessary to mention that I have no power of enforcement and cannot dictate whether covert surveillance powers should, or should not, be used. I neither promote nor limit the use of covert powers. My responsibility is limited to examining the processes that are used should a public authority decide to seek the protection that legislation affords'.

The Constitution Committee described this answer as 'unsatisfactory', however, on the basis that it was 'essential that the regulators overseeing the use of RIPA powers should maintain public confidence in the regime'. The Committee, therefore, recommended that the relevant oversight Commissioners under RIPA should:[523]

> introduce more flexibility to their inspection regimes, so that they can promptly investigate cases where there is widespread concern that powers under the Regulation of Investigatory Powers Act 2000 have been used disproportionately or unnecessarily, and that they seek appropriate advice from the Information Commissioner.

ANPR and CCTV

276. As we saw in the introduction, there has been a massive increase in the use of large-scale public surveillance in the UK over the past three decades, primarily through the use of CCTV. The lack of any overarching regulatory regime governing the use of CCTV was highlighted in the case of *Peck* before the ECtHR. At the same time, the issue in that case was whether the subsequent disclosure of the CCTV footage complied with the requirements of Article 8, not the more general absence of a legal basis for the prior surveillance. In light of ongoing public concerns, Chapter 1 of Part 2 of the Protection of Freedoms Bill provides for Code of Practice governing the use of surveillance cameras and this has been followed by a Home Office consultation on the same issue.[524]

277. Although public CCTV surveillance may undoubtedly give rise to serious interference with personal privacy, it largely falls outside the scope of 'directed surveillance' because: i) it is generally visible to the public and, therefore, not covert under section 26(9); and ii) it is not usually conducted 'for the purposes of a specific investigation or operation' under section 26(2).[525]

278. However, the targeted use of large-scale public surveillance systems such as CCTV or ANPR has become increasingly common over the last decade, to the growing concern of the Surveillance Commissioners. In 2005, for instance, inspections by the Office of the Chief Commissioner revealed 'increased strategic use of CCTV systems by public authorities for enforcement and security purposes'.[526] In his annual report that year, the Chief Commissioner reported, however, that his inspectors had not detected any use of ANPR 'that is incompatible with the legislation'.[527] By his 2006 report, however, it had become clear that the Surveillance Commissioners were alarmed by the growing use of ANPR:[528]

> ANPR has proved very effective in crime reduction and is a prime example of intelligence-led policing. But the deployment of an ANPR camera *constitutes surveillance when an identifiable image is recorded of a person in a vehicle.* It probably also amounts to the obtaining of private information about any such person, whether or not that person has been identified for the purposes of the investigation or operation. The procedure will, therefore, be vulnerable to challenge unless it is authorised.

---

523. N72 above, para 257.
524. Home Office, *Consultation on a Code of Practice relating to Surveillance Cameras.* In 2008, the Information Commissioner also issued a Code of Practice governing the use of CCTV, but this in relation to the provisions of the Data Protection Act rather than its use for the purposes of surveillance.
525. Section 26(2).
526. 2004-2005 report, para 14.4.
527. Sir Andrew Leggatt, *Annual Report of the Chief Surveillance Commissioner 2004-2005* (HC 444, November 2005), para 14.5.
528. Sir Christopher Rose, *Annual Report of the Chief Surveillance Commissioner 2005-2006* (HC 1298, July 2006), paras 14.1-14.5.

Although surveillance by a visible camera was not normally covert, the Chief Commissioner said, 'ANPR is not a normal case'. Even in cases where the road camera was visible, 'occupants of vehicles are unaware that the camera may make and record identifiable images of them'. Moreover, it would not be easy to provide effective notice since 'explaining the true purpose of the equipment briefly is not easy'. [529] The large-scale recording of data gathered by ANPR meant that 'it is unlikely that the deployment could be authorised under RIPA': [530]

> There may well be human rights issues arising in connection with any use of private information to build up pictures of the movements of particular persons or vehicles … *The unanimous view of the Commissioners is that the existing legislation is not apt to deal with the fundamental problems to which the deployment of ANPR cameras gives rise.* This is probably because the current technology, or at least its very extensive use, had not been envisaged when the legislation was framed. The Commissioners are of the view that legislation is likely to be required to establish a satisfactory framework to allow for the latest technological advances.

The Chief Commissioner, therefore, urged the Home Secretary to legislate to put the use of ANPR on a statutory footing. In his 2008 report, he referred to his disappointment 'at the apparent lack of momentum'.[531]

279. Although legislation has not been forthcoming, it may be no coincidence that, as of 2010, the Code of Practice now advises that:[532]

> where overt CCTV or ANPR cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people a directed surveillance *authorisation* should be considered. Such covert surveillance is likely to result in the obtaining of *private information* about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or ANPR system in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

280. At the same time, however, it is apparent that regulatory problems raised by ANPR have continued. In its recent consultation on a Code of Practice for surveillance cameras, for instance, the Home Office noted that:

> Like CCTV, the use of ANPR has developed in the absence of a specific statutory or regulatory framework leaving scope for ambiguity as to its purpose and usage. With the pace of development of technology, there is the potential for the use of ANPR to outgrow its original strategic aims.

529. Ibid.
530. Ibid.
531. 2007-2008 report, para 2.3. See also para 8.6: 'I will avoid the temptation to rehearse the arguments that I and my predecessor have presented over consecutive years for amendments that enable public authorities lawfully to take advantage of the opportunities that improvements in technology offer. I have declared that I would be sympathetic to amendments that provide greater clarity providing that the amendments remain compliant with the principles of the protection of privacy and human rights ... I am concerned by the apparent reluctance to make necessary amendments and at the suggestion made in some quarters that it would be more helpful if the Commissioners would change their opinions. I understand that the scope for amendment is to be considered later this year and I urge appropriate momentum'.
532. Code of Practice, para 2.28. Emphasis in original.

Although it noted that there were 'strict ACPO guidelines' on the use of ANPR by police, it conceded that:

> There is much less clarity around the use of ANPR by private companies, for example in monitoring private premises and car parks and how data is then used or exchanged with other parties. Whilst the Police Service has agreed standards for the quality of data it collects, no such standards exist for private companies. Private companies and individuals account for a substantial number of surveillance cameras in the UK.

281. In relation to these developments, the Chief Surveillance Commissioner has also expressed concern at public bodies using private operators to carry out surveillance, saying that it was 'clear' that:[533]

> many public authorities (including law enforcement agencies) are using private entities in one form or another (for example private investigators and ANPR product). My Commissioners have advised that when private enterprises are used to conduct covert surveillance on behalf of a public authority, *this fact should be clear in authorisations and the operators bound by the terms of the authorisation.*

282. The growing use of ANPR is just one instance of how the conventional (and itself quite recent) distinction referred to in Chapter 1 between 'active', covert surveillance targeting particular individuals, and 'passive', large-scale public surveillance directed at the world at large, has already begun to erode through the increasing sophistication of digital technology. Systems such as ANPR invert the traditional model of an investigator deciding to put a subject under surveillance and then carrying it out. With ANPR, the individual has already been under surveillance for some time; it is simply a matter of the investigator requesting and analysing the data that has already been automatically gathered. Similar definitional challenges are likely to arise from the increasing use of other surveillance technologies, such as aerial drones, with the capability to carry out both broad-based and targeted surveillance.

Recommendations

Revise definition of 'directed' surveillance

283. In line with our recommendation in Chapter 5 that the definition of 'intrusive' surveillance should be considerably extended, the definition of 'directed' surveillance should be correspondingly narrowed to cover any covert surveillance that seeks to obtain information about an individual but does not involve significant interference with their privacy (which we take to be the essential definition of intrusive surveillance). This would include, for example, using a surveillance device to overhear someone's conversation at a bus stop, or following their movements at work over a period of several days. Equally it would exclude any surveillance that is likely to result in any person acquiring knowledge of privileged material, confidential personal information or confidential journalistic material, etc.

---

533. 2010-2011 report, para 5.14. See also eg, 2008-2009 report, para 5.17: Use of private contractors by public bodies is covered by RIPA: 'I have also made it clear that those public authorities which use the services of private sector investigators render those investigators liable to inspection by me. When authorised to conduct covert surveillance using public funds they must comply with the legislation. This should be made clear during negotiations and by contract'.

284. In addition, the definition of directed surveillance should also include any plan to use overt surveillance, including CCTV or ANPR, in a targeted manner for the purposes of a specific investigation or the surveillance of a particular person. Associated with this, the Code of Practice for surveillance cameras proposed by the Protection of Freedoms Bill should be mandatory and apply to all surveillance cameras used by public and private bodies alike.

Improve authorisation and oversight

285. Internal authorisation of directed surveillance without prior judicial approval is only appropriate for the police and other law enforcement agencies with responsibility for investigating and prosecuting serious crime, and for whom the purpose of surveillance is obtaining admissible evidence. For these organisations, the possibility that evidence may be excluded by the judge at trial, combined with oversight of the Office of Surveillance Commissioners appears to be an adequate safeguard against abuse.

286. For the wide range of other public bodies able to use directed surveillance under Part 2 of RIPA, self-authorisation carries with it an unacceptable degree of risk that does not appear to be adequately checked by the Surveillance Commissioners. We, therefore, recommend that the proposal in clause 38 of the Protection of Freedoms Bill to introduce prior judicial approval for the use of directed surveillance should be extended to all other public bodies, other than the police and law enforcement agencies. Consistent with our recommendations in Chapter 5, we recommend that the language of application and approval should be replaced with the more straightforward process of the public body in question applying to a magistrate for a warrant for directed surveillance.

287. Since the use of directed surveillance by the intelligence services is self-authorised and is not generally subject to ex post facto review by a court, the oversight of the Intelligence Services Commissioner is the sole independent check that they are exercising their powers correctly. Unfortunately, the Commissioner's annual reports provide very little information upon which to be satisfied that he is providing an effective check. We, therefore, recommend that the intelligence services continue to be allowed to self-authorise directed surveillance, but that oversight for this should be transferred to the Chief Surveillance Commissioner, at least where it concerns the surveillance activities of the services within the UK.

288. Although effective regulation and oversight of mass surveillance systems such as ANPR and CCTV is sorely needed, the proposal in clause 34 of the Protection of Freedoms Bill to establish a Surveillance Camera Commissioner is misguided and would only add to the unnecessary proliferation of oversight bodies relating to RIPA. Instead, the Information Commissioner's office should have primary responsibility for regulation of surveillance cameras, with appropriate powers to enforce compliance. The Chief Surveillance Commissioner should continue to have oversight in relation to any surveillance system likely to be used for directed surveillance, however, particularly in relation to law enforcement.

Chapter 7
Covert human intelligence sources

289. The use of informants, paid and unpaid, and undercover officers has long been an essential feature of criminal investigations. At the same time, some regulation of the practice has always been thought desirable in order to ensure, in the words of Lord Hoffmann, that the police 'prevent and detect crime, not employ themselves in creating it'.[534]

290. Prior to RIPA, there was no legal framework in the UK governing the use of informants and undercover officers,[535] notwithstanding the increasingly high profile use of so-called 'supergrasses' in criminal trials in the 1970s and 80s. Aside from the obvious point that such covert sources are one way of obtaining private information about a person, and thereby required a sufficient basis in law under Article 8(2), the government was no doubt mindful of the implications of the 1998 judgment of ECtHR in *Teixeira de Castro v Portugal.* [536]

291. In *Teixeira* the applicant complained that he had only purchased heroin at the behest of two undercover police officers who had given him the money to purchase it. Distinguishing between those cases in which an undercover agent 'created a criminal intent that had previously been absent' and those in which 'the offender had already been predisposed to commit the offence',[537] the Court went on to warn that:[538]

> The use of undercover agents *must be restricted and safeguards put in place* even in cases concerning the fight against drug trafficking. While the rise in organised crime undoubtedly requires that appropriate measures be taken, the right to a fair administration of justice nevertheless holds such a prominent place … that it cannot be sacrificed for the sake of expedience. The general requirements of fairness embodied in Article 6 apply to proceedings concerning all types of criminal offence, from the most straightforward to the most complex. The public interest cannot justify the use of evidence obtained as a result of police incitement.

In the applicant's case, by contrast, the Court noted that 'the police officers had acted on their own initiative without any supervision by the courts'.[539] In determining whether their actions went

534. *R v Loosey* [2001] UKHL 53 at para 59.
535. There was some non-binding guidance produced prior to RIPA, however, including Home Office Circular 97/1969 and, shortly before RIPA was introduced, a Code of Practice for Undercover Officers.
536. (1998) 28 EHRR 101.
537. Ibid, para 32.
538. Ibid, para 36. Emphasis added.
539. Ibid. See also para 31.

'beyond that of undercover agents', it placed particular weight on the fact that the Portuguese government had 'not contended that the officers' intervention took place as part of an … operation ordered and supervised by a judge'.[540] Concluding that the officers had effectively instigated the applicant's offence, the Court held that he had been deprived of his right to fair trial from the very start.[541]

292. The use of covert sources under RIPA, however, extends beyond undercover officers to include any person who acts covertly in their dealings with others in order to obtain information for a public body.[542] Accordingly, it is one of the most common powers enjoyed by public bodies under RIPA, alongside the use of directed surveillance and access to communications data. The use of covert sources is often authorised alongside, and used in conjunction with, either directed or intrusive surveillance.

293. Part 2 defines a covert source as a person who establishes or maintains a personal or other relationship with a person with the 'covert purpose' of:[543]

a) covertly using the relationship to obtain, or provide another person access to, information; or

b) covertly disclosing information obtained by the use of the relationship, or as a consequence of that relationship's existence.

The common factor in both activities is that it is carried out 'in a manner … calculated to ensure' that one party to the relationship is unaware of either the purpose of the relationship or the fact of the disclosure.[544]

294. Section 29 provides for a public authority to authorise the use of a covert source in essentially the same manner as that for directed surveillance set out in Chapter 6, save that since the Policing and Crime 2009 Act, there are now additional requirements in relation to making arrangements for the source, including that there will 'at all times' be:[545]

a) a 'qualifying person' who will have day-to-day responsibility for dealing with the source and for the source's security and welfare;

b) another qualifying person who will have general oversight of the use made of that source; and

c) a qualifying person who will have responsibility for maintaining a record of the use made of that source.

---

540. Ibid, para 38.
541. Ibid, para 39.
542. Lord Brown, *Report of the Intelligence Services Commissioner for 2001* (HC 1244, October 2002), para 26: 'Covert human intelligence sources are essentially people who are members of or act on behalf of one of the intelligence services to obtain information from people who do not know that this information will reach the intelligence service'. See eg, *Annual Report of the Chief Surveillance Commissioner 2010-2011* (HC 1111, June 2011), para 5.15: 'However, the ease with which statutory criteria are met is often misjudged; a person, irrespective of motive, may be a CHIS if he uses a personal or other relationship to pass information to a public authority in a manner that is covert in relation to the person to whom the information refers. ...I take this opportunity to remind public authorities that the threshold set by Parliament is low and that there is significant risk in reliance on a person within the statutory definition of a CHIS who is not authorised'.
543. Section 26(8).
544. Sections 26(9)(b) and (c).
545. Section 29(4A), as amended by section 8 of the Policing and Crime Act 2009.

In 2010, moreover, the Home Office made an order requiring prior judicial approval from a Surveillance Commissioner (or the Secretary of State in the case of the intelligence services) where the authorisation includes activities involving conduct of a source, or the use of a source, to obtain, provide access to or disclose matters subject to legal privilege.[546]

295. The use of covert sources under RIPA is covered by a Code of Practice.[547] In addition, although there is a common authorisation process for directed surveillance and the use of covert sources, Parts 1 and 2 of Schedule 1 of RIPA distinguishes between the powers available to different public bodies so that, for example, some public bodies are able to use directed surveillance but not covert sources, eg, the Royal Pharmaceutical Society of Great Britain.

296. Oversight of the use of sources under Part 2 of RIPA is provided by the Chief Surveillance Commissioner (in relation to their use by police, law enforcement agencies, and other public bodies) and the Intelligence Services Commissioner (in relation to their use by MI5, MI6, GCHQ, and the activities of the Ministry of Defence and the armed forces outside the UK).

297. Between 2000 and 2011, there have been 43,991 covert sources recruited under Part 2 of RIPA. The proportion of covert sources recruited each year by non-law enforcement bodies such as government departments and local authorities varies, but averages about seven per cent of the total.[548]

The need for prior judicial authorisation

298. As has already been discussed at length in earlier chapters, there are obvious flaws in any authorisation procedure in which the main safeguard against a public body carrying out unjustified surveillance is a senior official from the same organisation. Even the most diligent official would struggle to remain objective, particularly if the organisation is under pressure to meet targets or achieve certain results. The same considerations that have already been identified in Chapter 6 in relation to the authorisation of directed surveillance apply with equal force to the authorisation of covert sources: the relevant officials sometimes show a poor understanding of the concepts of necessity and proportionality; officials sometimes accept the application presented to them with insufficient questioning; and so forth.

299. And the shortcomings of the oversight arrangements for directed surveillance are the same in the case of covert sources. Not only are all authorisations not inspected, most are not. Instead, due to pressure on the increasingly scarce resources of the Chief Surveillance Commissioner, authorisations for covert sources are dip-sampled by the inspectors (who are themselves not legally trained).[549] In evidence to the House of Lords Constitution Committee, the Chief Commissioner could not say whether the sample was adequate or not: ten per cent was one figure he suggested. Even less information is available concerning the approach of the Intelligence Services Commissioner, but there is nothing to suggest that his approach is any more robust.

546. Regulation of Investigatory Powers (Covert Human Intelligence Sources: Matters Subject to Legal Privilege) Order 2010 (2010/123), Art 3.
547. Home Office, *Covert Human Intelligence Sources: Code of* Practice (2010), provided by The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Codes of Practice) Order 2010 (2010/462).
548. Source: annual reports of the Chief Surveillance Commissioner.
549. See Chapter 5 above.

300. The fact that evidence obtained from the use of an improperly authorised covert source might be excluded by the judge at trial for unfairness is also sometimes cited as a further check against unjustified surveillance. This is mistaken. The discretion of judges under section 78 of PACE to exclude evidence unfairly obtained may be an excellent safeguard against an unfair trial, but it will do nothing to address the interference with privacy that has already taken place. Moreover, the Chief Surveillance Commissioner noted, most material from covert surveillance is not used at trial. It seems clear, then, that most authorisations for the use of covert sources under Part 2 of RIPA are not subject to any kind of independent check whatsoever, let alone an effective one.

301. In January 2011, a series of reports in the *Guardian* newspaper identified a man named Mark Kennedy as the undercover police officer who had infiltrated a group of climate change activists and who had been involved in organising the group's protest against Ratcliffe-on-Soar power station: something which had apparently not been disclosed to the lawyers representing 20 members of the group at their trial for conspiracy to commit aggravated trespass. It emerged that Kennedy was just one of several undercover officers with the National Public Order Intelligence Unit who had spent several years infiltrating environmental protest groups.[550] Kennedy's undercover activities alone are estimated to have cost the taxpayer more than £2.25 million.[551]

302. In February 2011, the President of ACPO, Sir Hugh Orde, gave a speech on undercover policing in which he made reference to Kennedy's case and accepted that it raised 'questions around proportionality'.[552] While he gave a staunch defence of undercover policing as an essential tactic in the fight against crime, he noted that when it came to the use of such officers, 'the service has been left to pre-event, to regulate itself:[553]

> Except in very limited circumstances currently, there is no external pre-authorisation of this form of intrusion – the level of authority *by law* rests at Superintendent rank. Within the police service we consider this specialist and high risk area of policing sufficiently important that our own guidelines, agreed through the Association of Chief Police Officers, state that a chief officer should authorise all undercover operations. That is, Commander, Chief Constable, or higher. *This is a point of contrast in the law with other forms of surveillance* - for example the Secretary of State must issue a warrant to intercept communications. And except in urgent cases, intrusive surveillance – requires the consent of a Surveillance Commissioner (who must hold or have held high judicial office) to become effective. Pre-authority is required.

303. In view of the difficult decisions that the police were faced with in complex cases, Sir Hugh argued, it was necessary to adopt a procedure that could 'ensure that a valuable and lawful tactic is deployed in a way that ensures the proportionality and legitimacy is fully considered and challenged, within a necessary legal standard'. He concluded that:[554]

> It seems to me that the starting point may be no different as for any other tactic we deploy. The trigger rests with the operationally independent and responsible senior

550. See eg, 'Undercover officer spied on green activists', the *Guardian,* 9 January 2011; see also eg, 'Spying on protest groups has gone badly wrong, police chiefs say', the *Guardian,* 19 January 2011.
551. See eg, the *Daily Mail,* Farce of the £2m eco-activist undercover police operation , 18 April 2011.
552. 'Undercover Policing and Public Trust: Speech to Liberty', 7 February 2011.
553. The 'very limited circumstances' Sir Hugh refers to are presumably those cases in which a covert source is authorised as part of an intrusive surveillance operation. Emphasis added.
554. Emphasis in original.

> officer who currently makes the final decision without reference to the outside world. The current system of retrospective inspection is, in my judgment, no longer sufficient to secure the confidence of right thinking people that such interference with citizens' rights (with its foreseeable collateral intrusion on many) is appropriate. *Therefore the only solution I can see must take the form of some independent pre-authority that is already a common feature in other areas of policing in this country.*

Noting that prior judicial approval was already well-established in relation to authorisations for intrusive surveillance and property, he suggested that 'an additional element of judicial oversight in keeping with our traditions of accountability to the rule of law, need not be over-bureaucratic and the benefit would far outweigh the additional administrative burden'. He also stressed that he was 'not talking here about low level examples of the use of undercover such as test purchases from the street corner drug dealer, but the far smaller number of cases of the type where public confidence issues may be engaged'. He went on to suggest that 'some lower level authorities could probably be made less burdensome to balance the load without reducing the oversight'.

304. In July 2011, the Court of Appeal quashed the convictions of the protestors, following revelations that their group was one of a number that had been infiltrated by Kennedy, and that the Crown Prosecution Service had failed to disclose this at their trial.[555] Among other things, the Lord Chief Justice found that Kennedy 'was involved in activities which went much further than the authorisation he was given, and appeared to show him as an enthusiastic supporter of the proposed occupation of the power station and, arguably, an agent provocateur'.[556]

305. As noted in Chapters 4 and 5, the use of covert sources by local authorities has been widely criticised as disproportionate and, in 2010, the Home Office review of Counter-terrorism powers recommended that authorisation for their use should be subject to prior judicial approval. This proposal has now been introduced by clause 38 of the Protection of Freedoms Bill.

Recommendations

Improve authorisation procedures and oversight

306. In line with the President of ACPO's plea for judicial oversight, we recommend that complex operations involving the use of undercover officers should be subject to authorisation by warrant issued by a Surveillance Commissioner or Circuit Court judge. In our view, the appropriate threshold should include not only privacy considerations under Article 8 ECHR but also fair trial considerations under Article 6 ECHR.

307. The proposals in clause 38 of the Protection of Freedoms Bill for prior judicial approval for covert source authorisations should be extended to all other non-law enforcement bodies. Only the police, law enforcement and intelligence agencies should continue to be able to self-authorise the use of covert sources. Oversight for the use of covert sources in the UK should pass entirely to the Chief Surveillance Commissioner.

555. *David Robert Barkshire and others v The Queen* (Court of Appeal Criminal Division, unreported, 20 July 2011).
556. Ibid, para 18.

Chapter 8
Encryption Keys

308. As computers for business and personal use became increasingly common in the 1990s,[557] so too did the use of electronic encryption for a variety of purposes, including online transactions, fraud protection, and other basic features of Internet security. Naturally enough, the police and intelligence services began to worry about the threat that encryption posed to their investigative capabilities. In 1996, the Department of Trade and Industry published a White Paper outlining proposals for the licensing of encryption services:[558]

> The licensing policy will aim to protect consumers as well as to preserve the ability of the intelligence and law enforcement agencies *to fight serious crime and terrorism by establishing procedures for disclosure to them of the encryption keys,* under safeguards similar to those which already exist for warranted interception under the Interception of Communications Act.

A DTI consultation paper the following year noted that although cryptography was 'important for the protection of privacy'; it could 'also be put to improper use such as hiding the illegal activities of *criminals and terrorists*'.[559] Legislation would, therefore, be introduced to 'provide that the Secretary of State may issue a warrant requiring a [provider of encryption services] to disclose private encryption keys … of a body covered by that warrant'.[560]

309. Yet another consultation paper in 1999 stressed the investigative challenges posed by the use of encryption:[561]

> A number of recent investigations into a variety of serious criminal offences in the UK have been hampered by the discovery that material which might otherwise assist the investigation, or be used in evidence, has been encrypted. The problem is increasing. Law enforcement agencies often try to 'crack' the encryption key. Although this is occasionally possible after considerable effort and expense, it is likely to become increasingly difficult – if not impossible – as the technology develops.

557. See eg, Adrian Shepherd, *Use of ICT among Households and Individuals* (Office of National Statistics, 2007) p3: 'In 1998/99, one-third (33 per cent) of households in the UK possessed a personal computer'.
558. Department of Trade and Industry, *Paper of Regulatory Intent concerning Use of Encryption on Public Networks* (June 1996). Emphasis added.
559. Department of Trade and Industry, *Licensing of Trusted Third Parties for the Provision of Encryption Services: Public Consultation Paper* (March 1997), para 36. Emphasis added.
560. Ibid, para 76.
561. Department of Trade and Industry, *Building Confidence in Electronic Commerce: A Consultation Document* (URN 99/642, March 1999) para 49. See eg, an estimate from the Serious Fraud Office that 'some form of encryption is encountered' in roughly half its cases (para 50).

In particular, the paper claimed, 'the widespread use of encryption' represents 'a serious threat to the effectiveness of interception as a valuable and legitimate tool for law enforcement, security and intelligence agencies'.[562]

310. Instead of a warrant, the 1999 consultation proposed to 'establish a power to require any person, upon service of a written notice, to produce specified material in a comprehensible form or to disclose relevant material (eg, an encryption key) necessary for that purpose'.[563] This power would only apply, however, 'to material which itself has been, or is being, obtained lawfully'.[564] The consultation paper was also keen to reassure readers that the only reason the government wanted to introduce the power to obtain encryption keys was to prevent the effectiveness of 'the existing statutory framework for law enforcement, security and intelligence agencies' from being 'significantly undermined'.[565] In particular, it stressed that the government 'does not intend to use the new measures to extend, either directly or indirectly, its intrusive surveillance powers'.[566]

311. Shortly after the consultation paper was published in March 1999, the government published a second White Paper containing a Draft Electronic Communications Bill,[567] which included the power to issue notices to require disclosure of encryption keys.[568] In response, JUSTICE and the Foundation for Information Policy Research issued a joint opinion which criticised the draft provisions on the basis that they were likely to breach Articles 6 and 8 ECHR. For instance:[569]

> Especially where the private key is handed over, the law enforcement agencies will be able to decrypt and read any message received by the addressee of the notice, irrespective of whether it is covered by legal professional privilege or not. Only once a message has been read will it be clear whether the material contained therein is privileged in any way or not. There is nothing in the draft Bill that provides for supervision by an independent judge in relation to the decryption of intercepted material.

Rather than proceed with the draft Bill, however, the government decided to consolidate its provisions on encryption key disclosure into its broader framework legislation on surveillance powers. This long-heralded power to issue notices, therefore, became Part 3 of RIPA.

312. Part 3 applies wherever a public body comes into the possession of encrypted material, 'or is likely to do so', whether through the execution of any warrant (including interception warrants under RIPA[570] and search warrants),[571] requests for communications data,[572] the exercise of some other statutory power,[573] or simply 'any other lawful means'.[574]

313. In order to issue a notice under Part 3, the public body in question must first have permission to do so. With the exception of encrypted material obtained by the police or the intelligence services

562. Ibid, para 58.
563. Ibid, para 64.
564. Ibid.
565. Ibid, para 53.
566. Ibid.
567. *Promoting Electronic Commerce* (July 1999, Cm 4417).
568. See clauses 10-13 of the Draft Bill.
569. Joint Advice on the Draft Electronic Communications Bill prepared by Jack Beatson QC and Tim Eicke for JUSTICE and FIPR, 7 October 1999: (www.fipr.org/ecomm99/ecommaud.html), para 20.
570. Section 49(1)(b).
571. See section 49(1)(a) and para 2 of schedule 2.
572. Section 49(1)(c).
573. Section 49(1)(d) and para 4 of schedule 2.
574. Section 49(1).

under a warrant from or with the authorisation of the Secretary of State,[575] permission to make a Part 3 notice can only be given by a judge.[576] In addition, the Code of Practice provides that no public body can seek this permission without the prior approval of the National Technical Assistance Centre (NTAC), part of GCHQ.[577]

314. Second, in order to issue a notice the investigator must reasonably believe that:

(a) there is an encryption key in someone's possession;[578]

(b) it is necessary to issue the notice either for the purposes of national security, preventing or detecting crime, for the sake of the economic well-being of the UK, or for '*securing the effective exercise or proper performance by any public authority*' of any statutory power or duty;[579]

(c) that it is proportionate to do so;[580] and

(d) it is not reasonably practicable for the investigator to decrypt the material in question without issuing the notice.[581]

Where these conditions are met, the investigator may issue a written notice 'to the person whom he believes to have possession of the key',[582] identifying the encrypted material, the grounds on which it is believed to be necessary, the form and manner of the disclosure of the decrypted material and the deadline for providing it.[583] Normally the disclosure of the decrypted information will be sufficient to discharge the obligation. In exceptional circumstances, however, Part 3 also provides the power for investigators to require disclosure of the key itself.[584] In either case, deliberate failure to disclose the required information is a criminal offence.[585] However, where it emerges that the person notified does not, in fact, have the key needed to decrypt the material in question, his obligation to comply with the notice can be discharged by providing all such information that is in his possession 'that would facilitate the obtaining or discovery of the key', or otherwise making it intelligible.[586]

315. Although the majority of RIPA came into force shortly after it was passed in 2000, the power to obtain encryption keys under Part 3 was not brought into force until October 2007.[587] This was accompanied by a Code of Practice governing the use of encryption keys.[588] In particular, the Code makes NTAC 'the lead national authority for all matters' relating to encryption key notices,[589] and the 'guardian and gatekeeper of the use of Part 3'.[590] In particular, the Code provides that no public authority may serve a Part 3 notice, or seek the necessary permission to do so, 'without the prior written approval of NTAC to do so'.[591]

---

575. Para 2 of Schedule 2.
576. Para 1 of Schedule 2.
577. Code of Practice, para 3.10.
578. Section 49(2)(a).
579. Section 49(2)(b).
580. Section 49(2)(c).
581. Section 49(2)(d).
582. Ibid.
583. Section 49(4).
584. Section 51.
585. Section 53.
586. Subsections 50(8)-(9).
587. Regulation of Investigatory Powers Act 2000 (Commencement No 4) Order 2007 (SI 2007/2196).
588. Home Office, *Investigation of Protected Electronic Information: Code of Practice* (2007).
589. Code of Practice, para 3.10.
590. Code, para 3.11.
591. Code of Practice, para 3.10.

316. Oversight of Part 3 notices is provided by no less than three different Commissioners: the Interception Commissioner in relation to encrypted interceptions and encrypted communications data;[592] the Intelligence Services Commissioner in relation to the activities of the intelligence services, the Ministry of Defence and members of HM forces under Part 3;[593] and the Chief Surveillance Commissioner in relation to any other uses of Part 3 notices.[594] Offences under Part 3 (failure to comply with a notice under section 53 and disclosing the existence of a notice to another under section 54) are dealt with by the ordinary criminal courts. The IPT has jurisdiction to hear complaints against public bodies about the use of Part 3 notices,[595] as well as exclusive jurisdiction over any damages claims arising from the unlawful disclosure of an encryption key by a public body.[596]

317. No figures have been published for the number of notices served between October 2007, when Part 3 came into force, and the end of March 2008. According to the Chief Surveillance Commissioner, though, NTAC has approved 90 applications for the service of a notice between April 2008 and 31 March 2011. Of these, 56 had permission granted by a Circuit Judge, and 49 have been served. However, these figures only appear to cover those notices within the remit of the Chief Surveillance Commissioner and do not include those relating to interceptions, requests for communications data, or the activities of the intelligence services.

Unnecessarily complex authorisation and oversight

318. Many parts of RIPA are poorly-drafted and unnecessarily complex. The provisions of Part 3 and Schedule 2, however, are especially abstruse. It is doubtful whether any useful purpose is served by devising a scheme of such complexity. Certainly, we can see no reason why the relevant law should need to be framed in this way. In any event, the extremely poor drafting of Part 3 gives rise to a number of problems.

319. First, it makes the law itself difficult to apply. As the Criminal Division of the Court of Appeal noted in 2008, the exercise of the power to give a notice under section 49 is:[597]

> subject to compliance with extensive pre-conditions which must be demonstrated to the satisfaction of a judge without whose permission the notice cannot be given.

Although we strongly welcome the role of prior judicial authorisation for notices, the unnecessary complexity of Part 3 increases the likelihood of a wrong decision; whether it is a judge refusing permission when she should grant it, or granting permission when she should refuse it. In either case, it gives rise to an unacceptable risk that the requirements of necessity and proportionality under Article 8(2) will not be met.

320. Second, the undue complexity of Part 3 makes it difficult for members of the public to foresee the conditions under which a public official may demand to see their encrypted material or, alternatively, when a public official may secretly require a third party to decrypt it without their

592. Section 57(2)(c) and (d)(ii).
593. Section 59(2)(b) and (c) of RIPA and para 11.3 of the Code of Practice.
594. Section 62(1)(b) and (c).
595. Section 65(5)(e).
596. Sections 55(4) and 65(3)(c).
597. *R v S and A* [2008] EWCA Crim 2177 at para 10.

knowledge. Under Article 8(2), the law must be 'sufficiently clear' as to give those subject to it an 'adequate indication' as to when such powers were likely to be used.[598] While this does not mean that members of the public must be able 'to foresee precisely' when decryption may be required,[599] the sheer complexity of Part 3 makes it challenging even for lawyers to interpret accurately. The ECtHR has repeatedly stressed the need for 'clear, detailed rules' governing interception, for instance, and it has also said there was no reason not to apply the same principles of 'accessibility and clarity' to 'more general programmes of surveillance'.[600]

321. Third, this lack of clarity is compounded by the extremely fragmented nature of the oversight under Part 3, spread across three different commissioners. This makes it correspondingly more difficult for members of the public to assess from their annual reports whether the relevant law is being correctly applied. This is particularly true given the general lack of transparency of the Interception Commissioner and the Intelligence Services Commissioner. For instance, only the Chief Surveillance Commissioner publishes statistics as to the number of authorisations for the use of Part 3 notices given by NTAC, the number of times a Circuit judge has granted permission, and the number of times a Part 3 notice has been served. Figures for the number of Part 3 notices served in relation to interceptions, requests for communications data, or the activities of the intelligence services remain unknown. This, in turn, reduces any possibility of effective democratic oversight of their overall use.

322. As noted earlier, we welcome the general requirement of prior judicial authorisation for the use of Part 3 notices under Schedule 2 of RIPA.[601] In our view, this is a fundamental safeguard against their unnecessary or disproportionate use by public bodies contrary to Article 8(2). It is particularly vital in circumstances where the Part 3 notice is not served on the person whom the encrypted material belongs to, but served instead on a third party who will be required to secretly decrypt it without the owner's knowledge.

323. In cases where a person is required by a Part 3 notice to provide the key to, or otherwise decrypt, his own material, by contrast, he will at least know that his privacy is being interfered with, enabling him to either bring a complaint to the IPT, apply for an interlocutory ruling or raise the necessary defence in any subsequent criminal proceedings. In cases where the person is being required to decrypt his own material, however, it is difficult to see why the public authority's application for a Circuit judge's permission should not be made inter partes, assuming that the material in question is already in the custody of the public authority (ie, preventing the person notified from simply destroying it). In such cases, we see no reason why the person affected should not be given the opportunity to challenge the public authority's decision at the permission stage, rather than pursue a complaint to the Tribunal or raise the issue in subsequent criminal proceedings. This would enable the Circuit judge to come to a more informed view as to whether requiring the affected person to make available his encrypted material would be a necessary and proportionate interference with his Article 8 rights.

324. Even more problematic, however, are the category of cases in which the approval of a Circuit Court judge is not required for a Part 3 notice to be issued, ie, cases involving encrypted interceptions, communications data, and the activities of the intelligence services. In those cases, there will be no assessment by an independent authority of the necessity and proportionality of the interference

598. *Malone,* n124 above, para 67 and *Khan,* n152 above, para 26.
599. See *Leander,* n154 above.
600. *Liberty and others,* n151 above, para 63.
601. However, prior judicial authorisation is not required in relation to notices made by the intelligence services or in relation to interceptions.

with a person's Article 8 rights. Instead this task will normally fall to the Secretary of State – someone who is plainly not sufficiently independent for the reasons set out at length in Chapter 3. Nor does it appear from the reports of the relevant oversight commissioners in such cases – the Interception Commissioner and the Intelligence Services Commissioner – that much time is devoted to considering questions of necessity and proportionality of Part 3 notices in these contexts. It may be, however, that they simply have not had any Part 3 notices to review. As Sir Peter Gibson noted in his 2010 report:[602]

> no notification of any directions to require disclosure in respect of protected electronic information has been given to me in 2010 and there has been no exercise or performance of powers and duties under Part III for me to review.

325. Unusually, the Code of Practice does provide that:[603]

> Should any Commissioner establish that an individual has been adversely affected by any *wilful or reckless failure* by any person within a public authority exercising or complying with the powers and duties under Part III of the Act he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him to effectively engage the Tribunal.

This provision is striking in at least two ways. First, it seems to be a rare attempt to make the role of the oversight commissioners more transparent and accountable, by requiring them to notify the individual affected and disclose 'sufficient information' about the breach to enable him to pursue a complaint to the Tribunal. There is no corresponding provision in any other Code of Practice relating to the exercise of surveillance powers, see eg, the Interception Code of Practice.

326. Second, and much less favourably, the threshold of 'wilful or reckless failure' by a public authority under Part 3 appears to set the bar for notification much too high. After all, a person is entitled to be notified not just when a public authority has acted 'wilfully or recklessly', but *whenever* a public authority has acted unnecessarily or disproportionately under Part 3 in circumstances that give rise to a breach of his or her rights under Article 8. This is especially important in the context of decryption notices that are issued to third parties without the knowledge of the person affected. A threshold of 'wilful or reckless' failure, by contrast, will not catch the many cases in which a public authority diligently but mistakenly believes that it is necessary or proportionate to serve a Part 3 notice.

Encryption and the fight against terrorism

327. Over the years, the fight against terrorism has proved to be one of the more consistent justifications offered by successive governments concerning the need for encryption key legislation. It was cited twice in the first White Paper on the issue in 1996,[604] and five times in the first consultation paper issued the following year.[605] The second consultation in 1999 made no less than 13 references to

602. *Report of the Intelligence Services Commissioner for 2010* (HC 1240, June 2011), para 33.
603. Para 11.4. Emphasis added.
604. Department of Trade and Industry, *Paper of Regulatory Intent concerning Use of Encryption on Public Networks* (June 1996).
605. Department of Trade and Industry, *Licensing of Trusted Third Parties for the Provision of Encryption Services: Public Consultation Paper* (March 1997).

terrorism, and warned that there were already 'terrorists in the UK using encryption as a means of concealing their activities'.[606] It gave the example of a 1996 police operation against 'several leading members of a Northern Irish terrorist group', which involved the seizure of 'computer equipment containing encrypted files'.[607]

328. In light of the increasing prominence of terrorism as a justification for encryption key legislation, therefore, the failure of the government to bring Part 3 of RIPA into force until October 2007 requires a certain degree of explanation, especially after the events of 9/11. As Sir Swinton Thomas, the Interception Commissioner, explained in his annual report for 2004:[608]

> Part III of RIPA is not yet in force. Part 3 provides for the acquisition of the means to access or decrypt protected electronic data. However, *the use of information security and encryption products by terrorist and criminal suspects is not, I understand, as widespread as had been expected when RIPA was approved by Parliament* in the year 2000.

Indeed, the government's delay became all the more surprising when, two weeks after the 7/7 bombings, ACPO called for the maximum period of pre-charge detention in terrorism cases to be raised from 14 days to 90 days, and cited, in particular, the challenges of computer encryption as one of the major reasons for their request. In addition, ACPO called for the creation of 'a new offence of not disclosing encryption keys':[609]

> Recent investigations have been made more complex by difficulties for investigating officers *in ascertaining whereabouts of encryption keys to access computers etc.* An amendment to part 3 of the Regulation of Investigatory Powers Act (RIPA) to make it an offence to fail to disclose such items would provide some sanction against suspects failing to cooperate with investigations.

329. In the months that followed, the various arguments for and against raising the pre-charge detention limit were thoroughly rehearsed in public debate. In particular, the House of Commons Home Affairs Committee took evidence from a wide range of witnesses, including several computer experts who disputed the police's claims about the difficulties posed by encryption.[610] The government and the police offered differing explanations as to the merits of Part 3 of RIPA. The head of the Metropolitan Police's Anti-Terrorist Branch, Peter Clarke, for instance, gave evidence explaining that he did not believe it would be effective:[611]

> What we are looking at here are people who have secreted or encrypted material on their computers who, if that material were to be found, would stand the possibility of perhaps facing 20 years' imprisonment. If the choice is between giving the key to us to find evidence which could potentially lead to them serving 20 years or refusing to give the key to us and potentially being liable to two years' imprisonment under Part 3 of RIPA, I think the choice is fairly clear which one you would take.

---

606. Department of Trade and Industry, *Building Confidence in Electronic Commerce: A Consultation Document* (URN 99/642, March 1999), p25.
607. Ibid.
608. *Report of the Interception of Communications Commissioner for 2004* (HC 549, November 2005), para 7. Emphasis added. In yet another dismal example of the oversight commissioners under RIPA cutting and pasting one another's material, c.f. the annual report of the Intelligence Service Commissioner for 2004 (HC 548, November 2005), para 7: 'However, the use of information security and encryption products by terrorist and criminal suspects is not, I understand, as widespread as had been expected when RIPA was enacted in the year 2000'.
609. ACPO press release, 'Chief Police Officers recommend changes to counter the terrorist threat', 21 July 2005. Emphasis added.
610. House of Commons Home Affairs Committee, *Terrorism Detention Powers* (HC 910, 3 July 2006), paras 55-63.
611. Evidence of Deputy Assistant Commissioner Peter Clarke to the House of Commons Home Affairs Committee, 28 February 2006, Q229.

By contrast, the Home Secretary Charles Clarke told the Committee:[612]

> The short answer is that this part of RIPA was conceived in the expectation that it would only be four or five years before all electronic communications and all stored electronic data would be routinely encrypted, and that, in fact, has not happened at the speed at which we anticipated when the RIPA bill was passed. There are a lot of reasons for that, and the technological change is moving very quickly indeed in the whole of the communications field. It is also the case that the abuse of encryption by terrorists and criminals has not taken place at the speed at which we thought it would when the RIPA bill was passed. The take-up of encryption software has been low because a lot of it is still very difficult to use properly.

The Home Affairs Committee concluded that 'encryption of data does not appear, for the time being, to be the problem in practice that had been feared'.[613]

330. Despite this, the problems posed by the use of encryption by suspected terrorists re-emerged as one of the key justifications given by the police and the government for seeking the limit from 28 days to 42 days in 2007 and 2008. In its options paper on various alternatives, for instance, the Home Office highlighted the amount of material seized by police during Operation Overt (the investigation of the Liquid Bomb Plot involving transatlantic airliners) in August 2006:[614]

> 200 mobile phones, 400 computers and a total of 8,000 CDs, DVDs and computer disks, containing 6,000 gigabytes of data, were seized.

331. Even after the defeat of the government's second bid to increase the pre-charge detention limit in 2008, the challenges of encryption in terrorism cases has continued to be cited by police as a major investigative issue justifying extended detention in terrorism cases. Giving evidence to the Joint Committee on the Draft Detention of Terrorist Suspects Bill in May 2011, Assistant Commissioners John Yates referred at length to encryption difficulties:[615]

> in the recent British Airways insider plot of which Rajib Karim was convicted, the Police Service faced a hugely complicated problem of encryption. The senior investigating officer at the end of the case said that it was an extraordinary case. I think that was 13 days, so they just got there in terms of the de-encryption, if you like. *You can envisage how terrorists will learn from these types of cases and that the encryption becomes more sophisticated. We hope that our expertise gathers pace with that, but you can never say so for certain, which is probably why it is wise to have the contingency* [to extend the maximum period of pre-charge detention in emergencies].

Similarly, in her speech on the government's counter-terrorism strategy in July, Home Secretary Theresa May cited the challenges of encryption as one of the reasons for seeking to legislate further:[616]

---

612. Evidence to the House of Commons Home Affairs Committee, Q326, 21 March 2006.
613. Home Affairs Committee report, n610 above, para 63.
614. Home Office, *Options for pre-charge detention in terrorism cases* (July 2007).
615. See eg, Evidence of John Yates, Assistant Commissioner, to the Joint Committee on the Draft Bill, 10 May 2011, Q326; see also eg, evidence of former Assistant Commissioner Andy Hayman to the Joint Committee, 3 May 2011, referring to Operation Crevice: 'It was a very difficult decision whether to charge or not. We were on a knife edge. We had sent these particular pieces of disc to the FBI, the CIA, GCHQ and others and they had had real difficulty encrypting them. Subsequently, they didófour to five months lateróand the evidence was there in a format that it certainly was not on the 14th day' (Q287).
616. CONTEST speech, 12 July 2011.

> As we seek to prosecute terrorists, we must also seek to maintain the intelligence coverage which leads us to their activity in the first place. Terrorists are increasingly using online technology, including Google Earth and Street View for attack planning. … The marauding attacks in Mumbai in 2008 were directed by people using off-the-shelf secure communications technology to stay in contact with each other. Software to encrypt mobile phone voice and text functions is widely available and improving. Peer-to-peer networks can be used to distribute files and information rapidly and securely. Cloud computing offers new means for storing, sharing and distributing material on-line. It can be encrypted and configured to work with mobile devices, leaving little or no trace of the data behind. To tackle these new and emerging threats our own technology must constantly evolve and adapt … Legislation will be brought forward to put in place the necessary regulations and safeguards to ensure that the response to this technological challenge is both proportionate and appropriate.

332. Given the continuing controversy about the challenges of encryption in terrorism cases, therefore, it is telling that the overwhelming majority of cases concerning the use of Part 3 do not concern terrorism. As the Chief Surveillance Commissioner noted in his annual report in 2010:[617]

> [The offence of] the possession of indecent images of children … is the main reason why section 49 notices are served. Other offences include: insider dealing, illegal broadcasting, theft, evasion of excise duty and aggravated burglary. *It is of note that only one notice was served in relation to terrorism offences.*

In his 2011 report, the Chief Surveillance Commissioner again listed the offences in which section 49 notices had been served: 'the possession of indecent images of children. Other offences include: domestic extremism, insider dealing, fraud, evasion of excise duty, drug trafficking and drug possession with intent to supply'.[618] It is possible that terrorism features more prominently in relation to Part 3 notices that relate to encrypted interception, communications data and the work of the intelligence services, which fall outside the remit of the Chief Surveillance Commissioner. If, however, Part 3 notices are used to any extent in these areas, it has never been mentioned in the annual reports of either the Interception Commissioner nor the Intelligence Services Commissioner.

333. Despite many years of claims by government that encryption key powers were needed in order to combat terrorism, the available evidence suggests that Part 3 has, in fact, been little used for this purpose. It also suggests that the problems of encryption in terrorism cases have been somewhat overstated. In any event, it is clear that extended pre-charge detention is a hopelessly disproportionate response to any problems caused by encryption. The explanation offered by Commissioner Peter Clarke to the Home Affairs Committee in 2005 is particularly unconvincing. The use of Part 3 notices serves two purposes: either the suspect complies, in which the material is decrypted, or he refuses, and thereby commits a criminal offence punishable by imprisonment. In either case, the use of a Part 3 notice would obviously reduce any investigative pressures brought about by a suspect's use of encryption. More generally, Part 3 of RIPA illustrates two serious failings of public policy over the last 15 years: the persistent and unnecessary resort of the government to terrorism as a justification for encryption key powers; and the equally unnecessary reliance of the police upon encryption difficulties when seeking to argue for the extended pre-charge detention of suspected terrorists.

---

617. *Annual Report of the Chief Surveillance Commissioner 2009-2010* (HC 168, July 2010), para 4.11. Emphasis added.
618. Ibid, para 4.12.

The right against self-incrimination

334. In our opinion on the encryption key provisions of the Draft Electronic Communications Bill in 1999, we highlighted the risk that requiring a person to disclose an encryption key might breach their privilege against self-incrimination, an implicit part of the right to a fair trial under Article 6 ECHR. As the ECtHR held in *Saunders v United Kingdom*:[619]

> the right to silence and the right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6. Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6 … The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused *without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused.* In this sense the right is closely linked to the presumption of innocence contained in Article 6(2) of the Convention.

In *Saunders*, the Court held that the privilege against self-incrimination was not absolute and, in particular, did not extend to 'material which may be obtained from the accused through compulsory powers but which have an existence independent of the will of the suspect', eg, documents acquired pursuant to a warrant, blood or DNA samples, etc.[620] In our 1999 opinion, we argued that the requirement to disclose a 'key' such as a password was not something which could be said to have 'an independent will of the suspect'. On the contrary, the purpose of the draft provisions was:[621]

> to obtain the private decryption key, which is very much in the mind of the suspect (at least via the password), to enable them to read a document they already hold (or are likely to hold). Any analogy with real evidence such as documents, blood or urine samples or undeveloped film is, in our view, inappropriate.

It is clear enough that, although the provisions of Part 3 are much more complex, they are similar in their general terms to the provisions of the draft Bill. The same arguments, therefore, apply. Nor are there any provisions in either Part 3 or the Code of Practice concerning the issuing of notices where the person affected asserts the privilege against self-incrimination.

335. This issue was considered by the Criminal Division of the Court of Appeal in 2008 in what appears to be one of a handful of terrorism cases involving a notice under Part 3.[622] The case concerned two men charged with conspiracy to breach a control order. Computers belonging to both men were found to contain encrypted material so notices were issued to require the production of the necessary keys. Following their refusal, both men were charged under section 53 of RIPA. Before trial, they made an interlocutory application to the Court of Appeal in which they argued that the Part 3 notice breached their privilege against self-incrimination.[623]

---

619. (1997) 23 EHRR 313, para 68. Emphasis added.
620. *Saunders v United Kingdom* (1996) 23 EHRR 313, para 69.
621. JUSTICE and FIPR opinion, para 37.
622. *R v S and A* [2008] EWCA Crim 2177.
623. Ibid, para 14: 'It is perhaps noteworthy that the submission assumes that the disclosure of the key to the protected data in the possession of the appellants would incriminate them, and indeed in the case of S, may provide evidence supportive of the prosecution case against him under section 58 of the Terrorism Act. There is no direct evidence before us that it would, and no admission to that effect has been made by the appellants. But we were invited to proceed on the basis for the purposes of this argument that if the appropriate key were provided, incriminating material may be discovered'.

336. Delivering the judgment of the Court, President of the Queen's Bench Sir Igor Judge rejected the argument that the password to the encrypted material did not exist independently from the will of the suspects:[624]

> On analysis, the key which provides access to protected data, like the data itself, exists separately from each appellant's 'will'. Even if it is true that each created his own key, once created, the key to the data, remains independent of the appellant's 'will' even when it is retained only in his memory, at any rate until it is changed … In this sense, the key to the computer equipment is no different to the key to a locked drawer. The contents of the drawer exist independently of the suspect: so does the key to it. The contents may or may not be incriminating: the key is neutral.

The President conceded, however, that the privilege against self-incrimination *could* be engaged in circumstances where the *fact* of a person's knowledge of the key itself might tend to incriminate him, eg, if it had already been proven that the only people who knew the password were members of a terrorist cell, etc.[625] The more important question, the President suggested, was 'if the privilege is engaged at all, is whether the interference with it is proportionate and permissible'.[626] Among other things he noted that the powers in Part 3 were for a legitimate objective ('to enable the otherwise unreadable to be read'); disclosure of the key itself did not constitute 'an admission of guilt', rather 'only knowledge of it may be incriminating'; the requirement under Part 3 was 'expressly subject to a proportionality test and judicial oversight';[627] and in the event of any unfairness it would always be open to the judge at trial to exclude the material under section 78 of PACE. Accordingly, 'neither the process, nor any subsequent trial can realistically be stigmatised as unfair'.[628]

337. The Court of Appeal's analysis was subsequently followed by the Divisional Court in *Greater Manchester Police v Andrews*,[629] concerning a convicted sex offender who was arrested on suspicion of having breached his Sexual Offences Prevention Order. Upon his arrest, his laptop and memory sticks were seized. A search of the laptops showed that the defendant had downloaded indecent material involving children but the memory sticks were encrypted. The police, therefore, sought the permission of the court to issue a Part 3 notice requiring the key. Although the defendant subsequently pleaded guilty, the Divisional Court was asked to rule whether – in a case where there was apparently 'no evidence to indicate whether or not the defendant does know what the key to the encrypted file is' – the privilege against self-incrimination was engaged:[630]

> because for the defendant to reveal what the key was, would itself be incriminating material, there being no other independent evidence to show that he does know what the key is.

The Divisional Court held, however, that to the extent that the defendant's privilege did arise, it was engaged 'only to a very limited extent' and that any interference with it was, therefore, proportionate.[631] In particular, McCoombe J noted that, in the circumstances, the assumption was

624. Ibid, para 20.
625. Ibid, paras 21-24.
626. Ibid, para 25.
627. Ibid. See also para 10: 'The exercise of the power however is subject to compliance with extensive pre-conditions *which must be demonstrated to the satisfaction of a judge without whose permission the notice cannot be given'*. Emphasis added.
628. Ibid.
629. [2011] EWHC 1966 (Admin).
630. Ibid, para 18.
631. Ibid, para 23.

that the defendant knew the encryption key to his own memory sticks 'was a perfectly legitimate inference to draw'.[632] The President Sir Anthony May concurred, noting that there were, in any event, 'a number of procedural safeguards against self incrimination at any subsequent trial which will very often and I think in this case, provide an entirely adequate safeguard'.[633]

338. If, however, the Court of Appeal's ruling is correct, a Part 3 notice which involves encrypted communications data or the activities of the intelligence services in which the privilege of self-incrimination is engaged is likely to breach Article 6 because of the relative lack of safeguards in such cases, specifically the lack of prior judicial authorisation.

Legal professional privilege

339. Part 3 makes no reference whatsoever to the possibility that encrypted material might be covered by legal professional privilege. It provides that any person served with a notice is entitled to obtain legal advice concerning the obligations it imposes,[634] but Part 3 is silent about those cases in which the material itself is privileged. Similarly, the only mention of it in the Code of Practice is by way of an indirect reference to 'confidential' material:[635]

> Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation, or to confidential business-client relationships where a disclosure requirement may be imposed upon a corporate body or firm.

As we noted in our 1999 opinion, however, it is only once a message has been read that it will be clear whether the material is privileged or not.

340. As we noted in Chapter 3 in relation to interception of privileged material, it is clear from the judgment of the Divisional Court in *In re C* and the House of Lords judgment in *In re McE* that any kind of surveillance of privileged communications requires prior judicial authorisation. The fragmentary nature of Part 3, however, means that this is not always required – particularly in relation to encrypted interceptions, communications data and the work of the intelligence services.

341. Even in those cases where permission from a Circuit Court judge is needed, however, the Code of Practice's reference to 'confidential' material is plainly inadequate as a guide to the interests at stake. By contrast, the Interception Code of Practice makes detailed reference to the possibility that intercepted material may contain privileged material. Consequently, there is a risk that a public authority applying ex parte to a Circuit judge for permission to serve a Part 3 notice may fail to highlight the correct issues.

342. Where material is clearly privileged, moreover, there is likely to be considerable conflict between the strict procedures for handling privileged material under PACE, for instance, and the marked generality of Part 3 of RIPA.

---

632. Ibid, para 21.
633. Ibid, para 28.
634. Sections 54(6) and (7).
635. Code of Practice, para 3.40.

Recommendations

Extend prior judicial authorisation to all cases

343. In our view, the requirement that any public authority must obtain permission from a Circuit judge before serving a notice under Part 3 is a fundamental safeguard against unnecessary or disproportionate interference with the privacy of the affected person. It is particularly important in those cases where the Part 3 notice is not served on the person whom the encrypted material belongs to, but on a third party who will be required to secretly decrypt it without the owner's knowledge. It is also essential in any case involving interference with legal professional privilege or the privilege against self-incrimination.

344. For these reasons, we recommend that the safeguard of prior judicial approval should be extended to *all* cases under Part 3, including those involving encrypted interceptions, communications data and the intelligence services. In these sensitive cases, however, permission to make a Part 3 notice should be obtained from a security-cleared Divisional Court judge rather than a Circuit Court judge.

345. In cases where a person is required by a Part 3 notice to provide the key to, or otherwise decrypt, his own material, we recommend that any application should be made inter partes to allow him to challenge the public authority's decision at the permission stage. This would enable the judge to come to a more informed view as to whether requiring the affected person to make available his encrypted material would be a necessary and proportionate interference with his Article 8 rights.

Rationalise oversight arrangements

346. In our view, the extremely fragmented nature of the oversight arrangements for Part 3 are plainly unsatisfactory. Consistent with our recommendations in other chapters, we recommend that the Chief Surveillance Commissioner assume oversight of all of Part 3. However, we expect that, with extending the requirement of prior judicial authorisation to all cases, the oversight burden will be significantly reduced.

347. We also recommend that the Code of Practice for Part 3 should be amended to:

i. require the Commissioner to notify any person that he establishes has been adversely affected by an *unnecessary or disproportionate decision* under Part 3 of RIPA. As before, the Commissioner should also disclose sufficient information about the decision to the affected individual to enable him to effectively engage the Tribunal; and

ii. better reflect the importance of legal professional privilege, the protection of journalistic sources, and the privilege against self-incrimination.

Chapter 9
The Investigatory Powers Tribunal

348. The origins of the IPT date back to the Interception of Communications Act 1985, section 7 of which provided for a Tribunal to investigate complaints from people who believed that their communications had been intercepted. The Tribunal was empowered to investigate whether or not an interception warrant had been made and 'applying the principles applicable by a court on an application for judicial review', decide whether the Secretary of State's decision was justified. Where the Tribunal was satisfied that a warrant contravened the requirements of the Act, it had the power to quash it and direct the Secretary of State to pay compensation. As the Home Secretary explained on the Bill's Second Reading, the provisions establishing the Tribunal were:[636]

> in many ways the most important of the Bill, and its full significance has perhaps until now not been fully appreciated. Therefore, I wish to take this opportunity to underline what [the provisions] do and what their significance is. They break completely new ground by providing an independent, powerful and effective means of redress if interception has been improperly authorised. A tribunal will be established consisting of five senior lawyers. They will be appointed by the Crown by letters patent for a fixed term. They may be removed from office only on an Address to the Crown from both Houses of Parliament. Those arrangements are, in substance, *the same as those which apply to the Ombudsman* and they secure the tribunal's complete independence.

The Home Secretary's analogy between the Tribunal and the Ombudsman was challenged by other members of the House, in light of the fact that the latter reports annually to Parliament.[637] The Home Secretary replied that the Tribunal was, in this sense, more analogous to a court:[638]

> in the sense that it is the individual who complains and if his complaint is upheld he will get proper redress in the form of the quashing of the warrant and the giving of compensation.

349. The Home Secretary's original reference to the Ombudsman was not entirely misplaced, however, as English courts traditionally have no inquisitorial or investigative function. As we first explained in our 1961 report on the Ombudsman system, the primary function of the Ombudsman is to 'act as the agent of Parliament for the purpose of safeguarding citizens against abuse or misuse

636. Hansard, HC Debates col 162, 12 March 1985. Emphasis added.
637. Ibid, Alan Beith MP, col 163.
638. Ibid.

of administrative power by the Executive'.[639] In particular, the Ombudsman is able to carry out investigations in a way that provides the necessary independence at the same time as it prevents undue disruption to the activities of the public body under investigation:[640]

> The accusatory character of complaints of maladministration has a special significance in relation to the machinery of investigation. As the Department is the object of the accusation, it follows that if the investigation is to be impartial, it should be conducted by some outside authority free from the real or apparent influence of the Department. *It is important, however, that the outside authority should not disturb the normal administrative processes of the Department more than is necessary for the purpose of investigating the particular complaint* and therefore it should conduct its investigation as informally as possible.

At the same time, however, the report noted that although the ultimate sanction of the Ombudsman system was 'the power to institute proceedings against civil servants', in practice 'the real sanction is the publicity which is given to the Ombudsman's criticisms of the Administration in his annual reports'.[641] As was noted by the Strasbourg Court in *Klass*, though, secrecy is essential to any effective system of covert surveillance. The Interception of Communications Tribunal was, therefore, designed to accommodate the government's longstanding policy of neither confirming nor denying whether interception had taken place. In particular, the complainant had no right to an oral hearing before the Tribunal and no right to disclosure of any of the other material that it might consider. As Lord Denning explained during debates on the Bill in the House of Lords:[642]

> *If* a person is worried that his telephone is being tapped, he has a machinery for remedy. He can go to the tribunal and ask for an investigation to be made to see whether his telephone is being tapped, lawfully or not. The tribunal will inquire into it. *It has to be done in the greatest confidence because we must not allow criminals or spies to get to know our means of communication or detection.* Those involved will do it in the greatest confidence and will detect any unlawful telephone tapping which is not authorised by the warrant. There is protection with recourse to the tribunal and afterwards, if need be, prosecution in the courts. *Throughout the Bill the important safeguard in all the inquiries is the security of the state. A lot of the inquiries must be completely secret, otherwise the criminals will get to know of our means of detecting them.*

Simply put, those who complained to the Tribunal would not be told that their communications were, in fact, subject to an interception warrant. They would only be told in the event that their complaint was upheld, ie, that there was a warrant and that the warrant was unjustified. In any other case, they would only be told that no breach of the 1985 Act had taken place.

350. In addition to not giving complainants reasons for its decisions, decisions of the Tribunal were not subject to review or appeal. As many members of the House pointed out during parliamentary debates, moreover, the Tribunal's investigative capabilities were restricted to determining whether or not an interception warrant had been made. It had no power to investigate unauthorised

639. *The Citizen and the Administration: the redress of grievances* (JUSTICE, 1961), p1.
640. Ibid, para 75. Emphasis added.
641. Ibid, para 100.
642. Hansard, HL Debates col 141, 9 July 1985. Emphasis added.

interceptions made without a warrant save to the extent that it was disclosed by the agencies themselves.[643]

351. The establishment of the Interception of Communications Tribunal was followed by the Security Service Act 1989, section 5 of which provided for 'a Tribunal for the purpose of investigating complaints about the Service'. Section 9 of the Intelligence Services Act 1994 provided for a similar tribunal to investigate complaints in relation to MI6 and GCHQ. The schedules to the 1989 and 1994 Acts required the tribunals to follow similar procedures to those adopted by the Interception of Communications Tribunals.

352. From 1986, when the Interception of Communications Tribunal began its work, until the enactment of RIPA in 2000, not a single complaint was ever upheld by any of the three tribunals charged with investigating complaints against wrongful interception or the activities of the intelligence services.

353. The IPT was established under Part 4 of RIPA to:

a. combine the functions of the three tribunals established under the 1985, 1989 and 1994 Acts, as well as the complaints function of the Surveillance Commissioners under the Police Act 1997;

b. hear complaints against *any* public body in respect of the exercise of its powers under RIPA, eg, directed surveillance, intrusive surveillance, requests for communications data and encryption key notices; and

c. exercise exclusive jurisdiction over all proceedings brought against the security and intelligence services under the Human Rights Act.[644]

Like its predecessor tribunals, the decisions of the Tribunal are not 'subject to appeal or liable to be questioned in any court',[645] with the exception of decisions relating to the jurisdiction of the Tribunal over directed or intrusive surveillance or the use of covert sources under Part 2. In addition, the Secretary of State has the power to expand the jurisdiction of the Tribunal by order.[646]

354. Like its predecessors, the Tribunal represents an attempt to combine the investigative functions of an Ombudsman with the judicial functions of a court. It is, for instance, under a statutory duty to investigate complaints.[647] It also has the power to quash warrants and authorisations as appropriate, order the destruction of any surveillance material, and award compensation.[648] Any official exercising powers under RIPA are under a statutory duty to disclose or provide the Tribunal with such information as it requires to carry out its functions.[649] In appropriate cases, it may also

643. Although he had previously noted that the inquiry by Lord Bridge of Harwich into interception of communications 'was not concerned with allegations that interception had taken place without the authorisation of the Secretary of State' (ibid, col 154), the Home Secretary nonetheless assured Parliament that he was satisfied that 'members of the security service did not carry out any interceptions without the authority of the Secretary of State' (ibid, col 155).
644. Section 65(2). See eg, *A v B* [2009] EWCA Civ 24, in which the Court of Appeal held that a judicial review of the Director of MI5's refusal to allow a former member of the MI5 to publish his memoirs could only be heard by the Tribunal.
645. Section 67(8).
646. Section 65(2)(d).
647. Section 67(3). See also *B v Security Service,* IPT/03/01/CH, 31 March 2003, para 28: The Tribunal 'is an independent body established to investigate the substance of such complaints. By virtue of its powers under [the 2000 Act] it is in a different position from an ordinary court or from other tribunals, such as the Information Tribunal, faced with a complaint about the holding of personal data and with an NCND response from the intelligence services to a request for access and disclosure. The Tribunal does not have to accept the NCND response as final or as preventing investigation of the facts by it'.
648. Section 67(7).
649. Section 68(6).

require the assistance of the relevant oversight Commissioner to assist in its investigations or to provide an opinion on any matter that fails to be determined by the Tribunal.[650]

355. Similarly, the Tribunal operates on essentially the same secret basis as its forerunners: there is no right to an oral hearing; no right to reasons for an adverse decision; no right to know the evidence put before the Tribunal by any other party; no right to cross-examine relevant witnesses; and no right of appeal or judicial review. As the Tribunal's own website puts it:[651]

> It is not the Tribunal's function to tell complainants whether their telephones have been tapped, or if they have been the subject of other activity. Its purpose is to ascertain whether legislation has been complied with and organisations have acted reasonably. If your complaint is upheld, the Tribunal may decide to disclose details of any conduct. If your complaint is not upheld, you will not be told if any conduct has been taken against you or not.

356. Between the beginning of 2001 and the end 2010, there have been 1,120 complaints concerning unwarranted or excessive surveillance by public bodies including the police and the intelligence services to the IPT.[652] The Tribunal, however, has only upheld 10 complaints in the past 10 years. Of these, six were upheld in 2010, five of which were individual complaints lodged by members of the same family concerning the unlawful surveillance carried out by Poole Borough Council in 2009.[653] In other words, there have been only six cases in the last decade in which the Tribunal has found surveillance by a public body to be unnecessary or disproportionate.

Lack of effectiveness

357. Since RIPA came into force in October 2000, there have been 2.7 million surveillance decisions that we know of. This does not include:

a) the number of interception warrants signed by the Foreign Secretary and Northern Ireland Secretary under RIPA;

b) the number of interceptions in prisons and secure mental health facilities; and

c) the number of communication data requests in 2004.

Given that the number of communications data requests averages about half a million a year, it seems certain that more than three million surveillance decisions have been made by public authorities under RIPA since October 2000.

358. Despite this, the IPT has only upheld 10 complaints against public bodies in the past decade, five of which arose from the same case. In other words, the success rate of complaints before the Tribunal

650. Section 68(2).
651. www.ipt-uk.com
652. Source: annual reports of the Interception of Communications Commissioner, Intelligence Services Commissioner and Chief Surveillance Commissioner.
653. *Report of the Interception of Communications Commissioner for 2010* (HC 1239, June 2011), para 9.4.

is about 0.5 per cent. By way of comparison, the Administrative Justice and Tribunals Council published a report in June 2011 entitled *Right First Time*. It noted that:[654]

> Every day, public bodies make thousands of decisions about individuals across a diverse landscape – welfare benefits, immigration, education, tax, health and so on. Unfortunately, *evidence suggests that far too many of these initial decisions are incorrect.* Across the public sector there are high volumes of appeals (more than a million each year) against decisions and complaints about service provision. A worrying proportion of these appeals and complaints – nearly 40 per cent in some cases – are upheld by tribunals or ombudsmen.

In particular, the Council noted evidence from successive reports of the National Audit Office which gave a 'conservative estimate' of approximately 1.4 million complaints against central government departments each year.[655] The Tribunal Service, in turn, recorded 793,900 complaints in 2009-2010.[656] These complaints, however, were thought to represent only the 'tip of the iceberg',[657] as the Council explained:[658]

> Many users of public services, who are often the most vulnerable in society, do not have the information, support or resources to pursue their case even when decisions are incorrect or a complaint would be justified. Others feel there is little point in doing so as it may not make any difference.

Despite these constraints, the Council expressed serious concern at the quality of decision-making at many public bodies:[659]

> Together with the high volume of cases going to appeal, the high success rate for appellants suggests a widespread failure by public services to get it right first time. The concerns of the NAO, select committees and standing committees as noted above are reflected in these appeal success rates. For example, in 2009-2010, 38 per cent of appeals made to the Social Security and Child Support tribunal were upheld, and in 2010 on average 27 per cent of appeals against the UK Border Agency were upheld.

In addition, the report noted, 'evidence also suggests that appeal success rates are even higher for appellants with legal representation'.[660]

359. In July 2011, JUSTICE made a Freedom of Information Act request to the HM Courts and Tribunals Service, seeking details of the number of cases received by the First Tier Tribunal (and its constituent predecessors) in the period from 2001 to 2011, broken down by the chamber, together with the number of successful outcomes in each case. Although the Service was unable to provide figures

654. Para 2. Emphasis added.
655. Ibid, para 17.
656. Ibid, Table 1, pg 13.
657. See Nick Wikeley, 'Future Directions for Tribunals: A United Kingdom Perspective', in R Creyke, *Tribunals in the Common Law World*, Sydney, The Federation Press, 2008, cited in the report, para 26: 'much administrative decision-making is hidden from public scrutiny. So, rather than as a pyramid or a ziggurat, it may be that the structure of initial decision-making and tribunals is better represented by the image of an iceberg – the visible upper tier, the (smaller) part of the iceberg, is above the waterline, while the mass of first instance decisionmaking in official agencies is hidden below the waterline and necessarily out of public view'.
658. *Right First Time*, n654 above, para 27.
659. Ibid, para 28.
660. Ibid, para 29.

for the last decade, the available figures for 2010 alone show success rates before different Tribunals and – by extension – a good indication of the general quality of decision-making by public bodies across a broad range of areas:[661]

Immigration and Asylum	41%
Criminal Injuries Compensation	44%
Social Security and Child Support	35%
Land Registry Adjudicator	14%
Mental Health	13%

The success rate of complaints before the IPT (six successful cases out of 1,115 = 0.5 per cent, or – to use the Tribunal's own statistics – 10 complaints upheld out of 1,120 = 0.9 per cent) is, by contrast, vanishingly small.[662]

360. There are two explanations for this astonishingly low success rate. The first is that the quality of decision-making by the hundreds of different public bodies able to use surveillance powers under RIPA is so high as to be virtually unassailable. To say that this seems unlikely is something of an understatement. It is, to put it simply, not credible.

361. After all, public officials in the UK daily make decisions on a very wide range of issues, some of which may affect only a single person, some of which may affect the entire country. The stakes may sometimes seem very low, eg, a consumer credit appeal or a planning application, or they may be momentous, involving the custody of a child, the reunification of a family, the availability of a particular medical treatment on the NHS, deportation to torture, the decision to send soldiers into battle, life and death. The point is that, even with the best will in the world, the most resources and the greatest diligence, all decision-makers make mistakes. And, as is well-known, public bodies in the UK do not always operate in ideal conditions, with sufficient resources, nor even sadly with the best will in the world.

362. This is true even when the stakes are relatively low but it is especially true when officials act under severe pressure, as is so often the case with the investigation of terrorism or other serious crime. In the US, following 9/11, this pressure led government officials to sanction such methods as the introduction of warrantless wiretaps, the waterboarding of detainees, and Guantanamo Bay. In the UK, this led to the maximum period of pre-charge detention being raised to 28 days, the introduction of indefinite detention without trial, control orders, and renewed attempts to deport suspects to countries such as Libya where the use of torture was well-known. These were but some of the measures approved by senior government ministers over the last decade: the same ministers, not incidentally, were also responsible for signing interception warrants and approving requests for the use of surveillance by the intelligence services. Yet, if we were to take the success

661. FOIA response of the HM Courts and Tribunal Service, dated 1 August 2011; see also eg, *Annual Tribunal Statistics, 1 April 2010-31 March 2011* (HM Court and Tribunal Service, 30 June 2011), Table 3.2 Social Security and Child Support Outcomes by Benefit Type 2010-11 and Table 4.2 Immigration and Asylum Outcomes by case type 2010-11.

662. This is lower even than the success rate for applications for judicial review against public bodies, which is a cause of action of last resort when all other avenues have been exhausted: see Ministry of Justice, *Judicial and Court Statistics 2010* (30 June 2011), p145: 'There were 16,300 applications for permission to apply for judicial review in the Administrative Court, a 24 per cent increase on 2009. Of these, around 10,500 were received, 5,200 applications were refused and 1,100 were granted. The majority of these applications, as in previous years, concerned asylum and immigration matters. There were 460 applications for judicial review which were dealt with in 2010, a six per cent decrease on 2009. Of these, 194 were allowed, 256 dismissed and 13 were withdrawn'. Assuming for the sake of argument that all 16,300 applications were dealt with in the same year (which will not be the case due to the overlap from year to year), this means that about 1.1 per cent of applications for judicial review were ultimately successful in 2010.

rate of complaints of the IPT as any kind of an indicator of the quality of surveillance decisions over the past decade, we would have to believe that – in a decade in which investigative pressures were sufficient to justify extended pre-charge detention and control orders – surveillance decisions somehow remained miraculously free of error.

363. Even in the absence of such investigative pressures, it beggars belief that public bodies and government departments that struggle to produce defensible decisions in the field of planning, pensions credits and incapacity benefits are somehow incapable of making mistakes when it comes to surveillance; that the same Home Office that averages less than a 60 per cent success rate when it comes to defending its decisions under the 1971 Immigration Act, somehow manages a 95.5 per cent success rate when it comes to RIPA.

364. The second and far more plausible explanation for the pitiful success rate of complaints before the IPT is that it is simply inadequate as a mechanism for protecting individuals against excessive or unnecessary surveillance by public bodies. First, the covert nature of surveillance combined with the absence of any ex post facto notification requirements –common to US law – means that in the overwhelming majority of cases, the subjects of unnecessary surveillance will never know that their privacy was unjustifiably invaded. It is telling, for instance, that the IPT's most notable success – the Poole Council case which accounts for a full 50 per cent of the complaints it has upheld over the last decade – was one in which the family was subsequently notified by the Council that they had been subject to surveillance.[663] Even people who appear to have strong grounds to suspect they have been the victims of unlawful surveillance frequently fail to pursue complaints. As John Yates told the Home Affairs Committee earlier this year:[664]

> **Chair:** So who told you this, that you were being hacked?
>
> **AC Yates:** From the methods I know that are used and the impact it has on your phone, your PIN number, I am 99% certain my phone was hacked during a period of 2005-06. Who by? I don't know, the records don't exist any more, but from the modus operandi that I know how it happens-
>
> **Chair:** Your phone was hacked between-
>
> **AC Yates**: -my phone was hacked, as have been a number of other people.

If the head of the counter-terrorism branch of the Metropolitan Police – an experienced investigator with substantial experience of surveillance and one with access to specialist legal advice – suspected his own phone was being hacked but took no steps to investigate it, it hardly seems surprising that ordinary people who may have equally strong suspicions that their own activities are being subject to surveillance may yet fail to pursue a complaint to the IPT.

365. Second, although public bodies are under a statutory duty to comply with the Tribunal's investigations, there is no indication that the Tribunal has any kind of investigative capability beyond the information supplied by public bodies. As noted above, the Tribunal can request the

663. N42 above, para 7: 'Only after the surveillance had been completed did the Council inform Ms Paton of the operation that had been covertly carried out over the period of 3 weeks'.
664. House of Commons Home Affairs Committee, *Unauthorised tapping into or hacking of mobile communications* (HC 907, 20 July 2011), Q353.

assistance of one of the oversight commissioners in appropriate cases. But the reports of the various commissioners show that this has only been used a handful of times in the last decade. And the commissioners themselves rely to a large extent on the cooperation of the agencies they supervise. This may be adequate when the issue is whether an authorisation or a warrant was necessary or proportionate, but it is plainly inadequate when the issue is whether a public body has carried out unauthorised surveillance in circumstances where, as Lord Neuberger noted in the *Binyam Mohamed* case, the agencies themselves have an interest in suppressing information that may indicate their wrongdoing. Certainly, if one were to rely solely on the reports of the Intelligence Services Commissioner, for instance, a reasonable person would have no reason to doubt the claims of the intelligence services that they always act lawfully. If the Tribunal is to be taken seriously as a credible and independent investigative body, it needs to demonstrate that its investigative capabilities extend beyond issuing requests for information to the relevant public body.

366. Third, the hopelessly secretive and unfair nature of the Tribunal's procedures means that even those complainants who reasonably suspect they have been victims of unnecessary surveillance are: i) very unlikely to pursue a complaint because it does not offer a reasonable prospect of success; and ii) if they do pursue a complaint, are very unlikely to succeed even if their case has merit. As the Administrative Justice Council report noted, most people 'do not have the information, support or resources to pursue their case', while others 'feel there is little point in doing so as it may not make any difference'.[665] If this is true of ordinary tribunals, where the average success rate is a relatively robust 25 per cent, it is not difficult to imagine how much more discouraged a would-be complainant would be to learn that his or her only recourse is a tribunal that does not guarantee an oral hearing, disclosure of relevant evidence, the opportunity to cross-examine relevant witnesses and is generally immune from judicial review or appeal. As the Council report noted, it is no coincidence that the success rate is higher where applicants before tribunals have legal representatives. We are bound to note that the success rate of applicants before the IPT would likely show a similar improvement in the event that it were to adopt anything like a remotely fair procedure.

367. To the Tribunal's credit, however, it did refuse an application by a public authority for an award of costs against a complainant whose complaint was withdrawn, resulting in preparation fees of £5,700 for an inter partes hearing. In February, the Tribunal concluded that it had no power to award costs in such circumstances, primarily on the basis that its 'primary task is to investigate the conduct of public bodies, and hence to be inquisitorial',[666] and that it appeared 'from the statute that the Tribunal was intended to be cost-free to the complainant'.[667] As the Tribunal's own website notes, its 'investigation of complaints and claims is free of charge'. This conclusion is to be welcomed: the prospects of complainants before the Tribunal are dim enough without the additional threat of an adverse costs order to dissuade them further.

368. Fourth, the low success rate of complainants before the Tribunal is bound to reflect the fact that it is essentially reactive, ie, it depends on complaints being brought by members of the public who suspect that they have been unlawfully surveilled. As the Strasbourg Court made clear in *Klass*, however, the secret nature of surveillance means that victims of excessive or unnecessary intrusion are unlikely ever to know that they are victims.[668] An unhappy corollary of this is that many people

665. See n658 above.
666. *W v A public authority* (IPT/09/134/C, 1 February 2011), para 9.
667. Ibid, para 8.
668. Or, as Lord Nueberger put it in *In re* McE [2009] UKHL 15, para 111, the secrecy of surveillance gives rise to 'two inherent paradoxical problems', one of which is that the authorities 'cannot warn the parties in advance that interception or listening in will or will not occur, as to do so would defeat the whole point of the exercise'.

who sincerely believe that they *are* subject to surveillance are not. Consequently, genuine victims almost never complain, while many of those who *do* complain often prove to be the ones whose suspicions are the least well-founded. This, in turn, gives rise to an unhealthy confirmation bias on the part of those authorities responsible for surveillance, in the sense that the miniscule success rate of complaints before the Tribunal – combined with the very limited oversight provided by the relevant commissioners in most cases – gives rise to a false sense of confidence that surveillance decisions under RIPA are overwhelmingly compatible with the Article 8 rights of those affected.

369. Although the ECtHR has accepted that the covert nature of surveillance gives rise to certain inherent problems for those unknowingly affected by its abuse or misuse, it has nonetheless tended to dismiss arguments highlighting the inadequate nature of oversight mechanisms. In *Klass*, for example, the Court said that:[669]

> In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue.

In its 1993 decision in *Christie*, moreover, the European Commission on Human Rights rejected a similar argument made concerning the UK mechanisms:[670]

> The fact that the Tribunals have never made a determination in favour of an applicant is insufficient, in the Commission's view, to indicate that the system of safeguards is not effectively functioning as intended by domestic law.

In our view, however, this is no longer a tenable position for the Court to adopt in respect of the UK. The extent of surveillance by public bodies over the past decade – approximately three million decisions under RIPA – combined with the pitiful record of the Tribunal – only six complaints upheld in ten years – means that it is impossible to take it seriously as an effective check against unnecessary surveillance. When measured against other administrative tribunals and in the light of poor quality decision-making by UK public authorities in general, no reasonable person could conclude that the IPT was adequate to the task.

Excessive secrecy and lack of procedural fairness

370. As we noted in our 2009 report *Secret Evidence*, the Tribunal's own procedures bear only a remote resemblance to any kind of open and adversarial system of justice. First, the Tribunal's overriding responsibility is not fairness to a complainant but to carry out its functions:[671]

> in such a way as to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services.

669. *Klass*, n138 above, para 59.
670. *Christie*, n155 above, para 63.
671. The Investigatory Powers Tribunal Rules 2000 (SI 2000/2665), rule 6(1).

Second, the Tribunal cannot disclose to a complainant the identity of any witness before it, any evidence it has received, or even the fact it has held a hearing without first having the consent of the person involved.[672] Third, the Tribunal is under no duty to hold hearings but any hearings it does hold must be in private.[673] In the event that a hearing is held, a complainant may have the opportunity to make submissions, give evidence or call witnesses.[674] However, there is nothing in the Tribunal's rules that *require* it to give complainants this opportunity. Nor are complainants entitled to an inter partes hearing, to be present when other parties give evidence or call witnesses.[675] Unlike proceedings before SIAC, there is not even provision for a special advocate to act for a complainant in relation to the closed material. Finally, complainants are only entitled to a reasoned judgment in the event that the Tribunal finds in their favour.[676]

371. In its first preliminary ruling in 2003, the Tribunal considered a challenge to its 'secretive and one-sided' rules of procedure.[677] The Tribunal accepted that the rule requiring all hearings to be held in private was ultra vires on the basis that there was 'no conceivable ground for requiring legal arguments on pure points of procedural law … to be held in private'.[678] The Tribunal also agreed that its preliminary rulings could be disclosed, whatever the outcome.[679] But it held that the other aspects of the Tribunal's procedures, including its sweeping restrictions on disclosure, were necessary in order to prevent breaches of the 'neither confirm nor deny' policy under which the intelligences services operated.[680]

372. Another preliminary ruling in 2004 in *B v Security Service* concerned an MP who had lodged a complaint to determine whether MI5 held 'personal data relating to his activities with ecological groups 15 or more years ago'.[681] The Tribunal considered how it could determine the issue without breaching the Security Service's 'neither confirm nor deny' policy. It ruled that B's right to privacy under Article 8 ECHR would only be engaged if the Security Service actually held data on B and that, even if it did, the Tribunal indicated that it might privately determine that the retention of the data was nonetheless justified under Article 8(2). In other words, B might only be entitled to know if his personal data was being held by MI5 in a way that amounted to a violation of Article 8(2), not whether it held it justifiably or if it even held it at all.[682]

373. In the case of *R (A) v Director of Establishments of the Security Service*, a former MI5 officer challenged the refusal of its director to grant him permission to publish his memoirs, alleging among other things that this was an unjustified interference with his right to free expression under Article 10 ECHR.[683] At first instance, the Administrative Court held that section 65(2)(a) of RIPA did not oust the jurisdiction of the High Court to judicially review the decisions of the director of MI5, as was contemplated by the House of Lords in *R v Shayler*.[684] This conclusion, however, was overturned

672. Ibid, rules 6(2)-(4).
673. Ibid, rules 9(2) and (6).
674. Ibid, rule 9(3).
675. Ibid, rule 9(4), which allows for 'separate oral hearings'.
676. Ibid, rule 13(2): 'When they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact'.
677. IPT/01/62 and PIT/01/77, 23 January 2003, para 146.
678. Ibid, para 171. See also para 172: 'The public, as well as the parties, has a right to know that there is a dispute about the interpretation and validity of the relevant law and what the rival legal contentions are'.
679. Ibid, para 190.
680. See eg, para 161.
681. *B v Security Service,* IPT/03/01/CH, 31 March 2003, para 3.
682. Ibid, para 39.
683. [2008] EWHC 1512.
684. [2002] UKHL 11 at para 31 per Lord Bingham.

by the Court of Appeal.[685] In its December 2009 judgment in the matter, the UK Supreme Court considered the extent of the Tribunal's jurisdiction to hear claims under HRA 1998 in relation to the intelligence services.[686] It also heard argument, though did not decide the point, concerning the general compatibility of the Tribunal's procedures with the right to a fair trial under Article 6 ECHR. In his judgment for the Court, Lord Brown referred to:[687]

> the self-evident need to safeguard the secrecy and security of sensitive intelligence material, not least with regard to the working of the intelligence services. It is to this end, and to protect the "neither confirm nor deny" policy (equally obviously essential to the effective working of the services), that the Rules are as restrictive as they are regarding the closed nature of the IPT's hearings and the limited disclosure of information to the complainant (both before and after the IPT's determination).

Among other things, Lord Brown noted that the European Commission of Human Rights in its 1993 decision of *Esbester v United Kingdom* had rejected arguments 'as to the form of proceedings adopted by the Security Service Tribunal and the Interception of Communications Tribunal, not least as to the absence of a reasoned determination'.[688] He concluded that he was:[689]

> wholly unpersuaded that the hearing of A's complaint in the IPT will necessarily involve a breach of article 6. There is some measure of flexibility in the IPT's rules such as allows it to adapt its procedures to provide as much information to the complainant as possible consistently with national security interests. In any event, of course, through his lengthy exchanges with B, A has learned in some detail why objections to publication remain. Article 6 complaints fall to be judged in the light of all the circumstances of the case. We would, it seems to me, be going further than the Strasbourg jurisprudence has yet gone were we to hold in the abstract that the IPT procedures are necessarily incompatible with article 6(1).

More generally, Lord Brown noted, even if the Tribunal's rules and procedures *were* incompatible with Article 6, 'the remedy for that lies rather in *their* modification than in some artificially limited construction of the IPT's jurisdiction'.[690] Noting the anomaly that, were A to press ahead with publication, any injunction against him would be dealt with by the ordinary courts under principles of open justice, in which he would be free to assert his Convention rights, Lord Brown raised the spectre that 'more, rather than fewer, proceedings involving the intelligence services should be allocated exclusively to the IPT'.[691]

374. In the 2010 case of *Kennedy v United Kingdom*, a chamber of the ECtHR considered a challenge to the Tribunal's compatibility with Article 6 (the right to a fair hearing) and 8 (the right to privacy).[692]

---

685. [2009] EWCA Civ 24. See eg, Laws LJ at para 22: 'It is elementary that any attempt to oust altogether the High Court's supervisory jurisdiction over public authorities is repugnant to the constitution. But statutory measures which confide the jurisdiction to a judicial body of like standing and authority to that of the High Court, but which operates subject to special procedures apt for the subject-matter in hand, may well be constitutionally inoffensive. The IPT, whose membership I have described, offers with respect no cause for concern on this score. And as I have noted the Rules have been held by the IPT to be Convention compliant save for paragraph 9(6) which has accordingly fallen away'. See also Lord Brown at para 23: 'Parliament has not ousted judicial scrutiny of the acts of the intelligence services' but rather had 'simply allocated that scrutiny ... to the IPT'.
686. [2009] UKSC 12.
687. Ibid, para 14.
688. Ibid, para 27. See also eg, 1993, 18 EHRR CD 72, 74.
689. Ibid, para 30.
690. Ibid, para 31. Emphasis in original.
691. Ibid, para 34.
692. (Application no. 26839/05, 18 May 2010) para 11.

The applicant, Kennedy, had been convicted of murder but had had his conviction overturned on appeal, and was subsequently convicted of manslaughter at a second retrial. Following his release from prison, he became concerned that his mail, telephone and emails were being intercepted, and lodged a series of complaints with the Tribunal. Among other things, he asked for an oral hearing in public; mutual disclosure of evidence between the parties; oral evidence of all witnesses being open to cross-examination by the other parties; and a reasoned decision from the Tribunal on each issue. Kennedy's case, thereby, became one of the bases of the Tribunal's first preliminary rulings.[693] Following the rejection of his substantive complaint in 2004, Kennedy complained to Strasbourg, alleging that Part 1 of RIPA failed to provide sufficient clarity as to when he would be subject to interception and that 'other procedural safeguards in place including the possibility of launching proceedings before the IPT, were, in the applicant's view, also inadequate to protect against abuse'.[694]

375. The Court, for its part, rejected Kennedy's claim that Part 1 of RIPA failed to provide an adequate indication of 'the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures', holding that the nature of offences which might give rise to interception were 'sufficiently clear'.[695] It referred to the reports of the Interception Commissioner and his 'biannual review of a random selection of specific cases' as an 'important control on the activities of the intercepting agencies and of the Secretary of State himself'.[696] Most significantly, the Court placed considerable weight upon the 'extensive jurisdiction' of the IPT to examine 'any complaint of unlawful interception', and its status as 'an independent and impartial body, which has adopted its own rules of procedure', and with powers to demand material from appropriate agencies, and quash interception warrants if necessary.[697] Accordingly, the Court concluded that there was:[698]

> no evidence of any significant shortcomings in the application and operation of the surveillance regime. On the contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors which accidentally occur … Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the [Tribunal], the impugned surveillance measures, insofar as they may have been applied to the applicant in the circumstances outlined in the present case, are justified under Article 8(2).

376. Turning to Kennedy's claim about the unfairness of the Tribunal's procedures, the Court said the 'need to keep secret sensitive and confidential information' concerning surveillance measures 'justifies restrictions'.[699] The central question was, therefore, whether the particular restrictions 'taken as a whole, were disproportionate or impaired the very essence of the applicant's right to a fair trial'.[700] It accepted essentially without question the government's claims that:[701]

---

693. See n677 above.
694. N692 above, para 131.
695. Ibid, para 159.
696. Ibid, para 166.
697. Ibid, para 167.
698. Ibid, para 169. Significantly, however, the Court's reasoning did *not* specifically address the applicant's complaint concerning the role of the Secretary of State under Part 1 of RIPA: 'As to the safeguards and the arrangements put in place by the Secretary of State under section 15 RIPA, the applicant contended that there was a circularity in the fact that the person responsible for issuing warrants was also responsible for the establishment of the safeguards' (ibid, para 134).
699. Ibid, para 186.
700. Ibid.
701. Ibid, para 187.

> it was not possible to disclose redacted documents or to appoint special advocates as these measures would not have achieved the aim of preserving the secrecy of whether any interception had taken place.

The Court also reiterated that the duty to give reasons 'may vary according to the nature of the decision and must be determined in the light of the circumstances of the case'. In the context of the government's commitment to the 'neither confirm nor deny' policy – which the Court again accepted without question – the Court agreed that this policy:[702]

> could be circumvented if an application to the [Tribunal] resulted in a complainant being advised whether interception had taken place. In the circumstances, it is sufficient that an applicant be advised that no determination has been in his favour.

Accordingly, the Court ruled, 'the restrictions on the procedure before the IPT did not violate the applicant's right to a fair trial'.[703] In particular, it found that:[704]

> In order to ensure the efficacy of the secret surveillance regime, and bearing in mind the importance of such measures to the fight against terrorism and serious crime, the Court considers that the restrictions on the applicant's rights in the context of the proceedings before the IPT were both necessary and proportionate and did not impair the very essence of the applicant's Article 6 rights.

As a result of the Court's ruling in Kennedy, the website of the Tribunal now claims that 'all Tribunal procedures' have been accepted by the ECtHR.

377. The ultimate compatibility of the Tribunal and RIPA as a whole with the requirements of Articles 8 and 6 of the Convention remains very much in doubt, however. *Kennedy*, it should be noted, is only a chamber judgment and, like any such judgment, is, therefore, liable to be subsequently reversed by a judgment of the Grand Chamber. More to the point, there are compelling grounds for the view that *Kennedy* was wrongly-decided, not the least of which was the Court's unquestioning acceptance of the Interception Commissioner's assurances that all was well, and its faith in the capacity of the Tribunal to effectively check abuse of surveillance powers by public authorities notwithstanding considerable evidence to the contrary. In the wake of serious concerns about the conduct of the intelligence services in relation to the torture of suspects abroad, for instance, a Commissioner who apparently spends two days a year looking at a small dip sample of the warrants of each agency is hardly a credible check against abuse. Neither is a Tribunal whose own investigative capabilities appear to be equally limited.

378. As to the government's arguments against the appointment of special advocates before the Tribunal, we see no reason why the Tribunal could not appoint security-cleared counsel to act as investigating counsel to challenge the public authority's surveillance decision in each case. As we detailed in our 2009 report, this is a standard feature in the ex parte authorisation of surveillance warrants in Queensland through the office of the Public Interest Advocate. A similar system has operated in Sweden for many years. Certainly it does not appear that the number of complaints dealt with by the Tribunal each year would make this unworkable. Moreover, if, as appears to be

702. Ibid, para 189.
703. Ibid, para 190.
704. Ibid.

suggested in some quarters, the Tribunal deals with a large number of unmeritorious complaints, then the workload of independent counsel would be correspondingly light.

379. More generally, the Court's assessment of the compatibility of the Tribunal's procedures with Article 6 is very much at odds with its conclusion in *Klass*:[705]

> the question whether the decisions authorising such surveillance under the [German statute] are covered by the judicial guarantee set forth in Article 6 … must be examined by drawing a distinction between two stages: that before, and that after, notification of the termination of surveillance. *As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned,* within the meaning of Article 6 … as a consequence, *it of necessity escapes the requirements of that Article.*

The analysis in *Klass* that surveillance decisions escape the guarantees of Article 6 ECHR for as long as they remain secret is surely the better view. It can only be once a person has been notified of a surveillance decision that the requirements of a fair hearing come into play.

380. The unfortunate influence of the flawed decision in *Kennedy* is clear from the judgment of the UK Supreme Court in *Tariq v Home Office*.[706] That case, heard alongside *Al Rawi*, concerned the withdrawal of Mr Tariq's security clearance to work as an immigration officer following the arrest of his brother and his cousin in the Liquid Bomb plot in August 2006. As the Supreme Court noted, there was no information to suggest that 'Mr Tariq had himself been involved in any terrorism plot'.[707] Nonetheless his clearance was withdrawn and his appeal to the Security Vetting Appeals Panel was denied. He, therefore, brought an employment claim alleging discrimination on the grounds of race and/or religion. In response, the Home Office sought to rely extensively on closed material in order to defend the claim. Mr Tariq's appeal to the Supreme Court, therefore, raised the issue of the compatibility of closed proceedings before the Employment Tribunal with the requirements of Article 6 ECHR.

381. In particular, the majority of the Supreme Court relied heavily on the judgment of the Strasbourg Court in *Kennedy* to support its conclusion that Mr Tariq's right to a fair hearing under Article 6 did not entitle him to disclosure of any details of the case against him, sufficient to enable him to give effective instructions to the special advocate representing him in closed proceedings – what Lord Brown referred to as 'A-type' disclosure after the 2009 judgment of the ECtHR in *A and others v United Kingdom*[708] and affirmed by the House of Lords in *AF (No 3)*.[709] As one member of the majority, Lord Brown, said of *Kennedy*:[710]

> There could hardly be a clearer example of a procedure being held compliant with article 6 notwithstanding the conspicuous absence of anything approaching A-type disclosure.

705. N138 above, para 75.
706. [2011] UKHL 35.
707. Ibid, para 5. See also eg, para 90: 'What is suggested, however, is that he could be vulnerable to pressures from someone in his community to abuse his position as an immigration officer'.
708. (2009) 49 EHRR 29.
709. [2009] UKHL 28.
710. [2009] UKSC 11, para 89.

Lord Dyson similarly noted:[711]

> *Kennedy* is a striking decision. But for the security issues raised in the case, it is surely inconceivable that the court would have concluded that the restrictions on the applicant's rights before the IPT (a completely closed procedure without even the protection of a special advocate) were necessary and proportionate and did not impair the very essence of the applicant's article 6 rights.

382. In a stirring dissent from the majority's judgment, however, Lord Kerr set out the defects of the Court's approach to Article 6 ECHR in *Kennedy*. His starting point was that the essence of a person's right to a fair hearing is that:[712]

> a party is entitled to know and effectively challenge the case made against him. Equality of arms, or a properly set adversarial contest, requires that both parties have equal, or at least a sufficient, access to the material that will be deployed against them. The adversarial contest sets the context and the adversarial contest arises in relation to article 6 rights as opposed to other Convention rights

Accordingly, Lord Kerr explained, cases involving Article 6 are distinguishable from cases such as *Leander* which do not involve questions of equality of arms or adversarial contest but only the interference with privacy under Article 8.[713] In *Kennedy*, however, the Tribunal had held that the applicant's Article 6 rights were engaged. As Lord Kerr notes, that finding 'was somewhat diffidently contested before the ECtHR', and it was 'not contended, as it might well have been, that article 6, according to the court's constant jurisprudence, did not apply to cases of surveillance.' The Strasbourg Court, therefore, proceeded 'on the assumption that article 6 did apply'.[714] As he noted:[715]

> the court's decision seems largely to have been influenced by the argument advanced on behalf of the government that it was simply not possible to produce the information that the applicant sought because national security would inevitably be compromised. That stance is entirely consistent with the view that surveillance cases do not engage article 6. It is surprising that more was not made of this by the government and that the court did not address the issue directly. If it had done and if it had followed its own constant jurisprudence, the anomaly, which I believe the decision in *Kennedy* represents, would have been avoided.

By contrast, referring to *Klass*, Lord Kerr concluded that the logic of the Court's position in that case was 'inescapable':[716]

> The entire point of surveillance is that the person who is subject to it should not be aware of that fact. It is therefore impossible to apply article 6 to any challenge to the decision to place someone under surveillance, at least until notice of termination of the surveillance

711. Ibid, para 154.
712. Ibid, para 124.
713. Ibid.
714. Ibid, para 125.
715. Ibid, para 126.
716. Ibid, para 128.

> has been given … It is precisely because *the fact* of surveillance must remain secret in order to be efficacious that article 6 cannot be engaged. It appears to me, therefore, that the decision in *Kennedy* ought to have been made on the basis that article 6 was not engaged because the issues that the case raised were simply not justiciable.

383. In our view, the reasoning of Lord Kerr is plainly correct. It cannot sensibly be said that the procedures of the IPT – in which there is no right to a hearing, no right to disclosure of relevant evidence, no right to know let alone cross-examine the testimony of adverse witnesses, and no right to any kind of reasons – are fair, at least without making a mockery of the very concept of procedural fairness. It would be more accurate, not to mention more intellectually honest, to instead endorse what was said in *Klass*: that secret surveillance decisions remain outside the scope of Article 6 ECHR for as long as they remain secret. As Lord Kerr said, there is otherwise:

> no principled basis on which to draw a distinction between the essence of the right to a fair trial based on the nature of the claim that is made. A fair trial in any context demands that certain indispensable features are present to enable a true adversarial contest to take place.

384. For his part, Lord Brown took the opportunity afforded by his judgments in *Tariq* and *Al Rawi* to again float the idea that the jurisdiction of the IPT might be widened to include other categories of cases:[717]

> In my judgment in *R (A) v Director of Establishments of Security Service* … I expressly contemplated that in certain circumstances the IPT's exclusive jurisdiction might with advantage be widened. True, I was not considering a case like the present. I seriously wonder, however, whether it might not be wise to channel all disputes arising in security vetting cases to a single tribunal – if not the IPT itself, then a body sharing some at least of its characteristics.

385. We very much doubt, however, that the problems caused by the excessive secrecy surrounding matters relating to national security will be solved by sending yet more cases to the IPT. For it is plain that the Tribunal is itself an unhappy compromise: a body vested with the investigative functions of an Ombudsman and the judicial functions of a court, but tasked at the same time with keeping secret the activities of the public bodies it investigates. The fundamental problem, as we identified in our 2009 report *Secret Evidence*, is that secrecy is ultimately incompatible with fairness and fairness is inherent in the very concept of a court. Practices such as the giving of reasons, or disclosure of relevant evidence to all the parties to a case are not incidental aspects of legal procedure: they are an essential part of the judicial function. It is true that the Tribunal is more inquisitorial than most English courts (although to judge by the rulings that have been published so far, its proceedings are still largely adversarial) but as Lord Justice May said concerning the 7/7

---

717. *Tariq*, para 94. See also Lord Brown's judgment in *Al Rawi*, para 86 'For my part I have reached the reluctant conclusion that, by their very nature, claims of the sort advanced here, targeted as they are principally against the Intelligence Services, are quite simply untriable by any remotely conventional open court process. The problems they raise, of oral no less than documentary evidence, are just too deep-seated to be capable of solution within such a process. Far too little would be gained, and far too much lost, by the appellants' proposed development of the common law. In short, some altogether more radical solution is, I believe, required. Realistically there seem to be only two possible solutions. Either cases of this kind, necessarily involving highly sensitive security issues, should go for determination by some body akin to the Investigatory Powers Tribunal which does not pretend to be deciding such claims on a remotely conventional basis (see my judgment in *Tariq v Home Office*). Or they must simply be regarded as untriable and struck out on the basis that, as Laws LJ put it in *Carnduff* at para 36: '[They] cannot, in truth, be justly tried at all'.

inquest, the fact that proceedings are inquisitorial 'does not diminish their context as essentially judicial procedures which are governed by the principle of open justice'.[718] Or as Lord Brown put it in a 2007 appeal:[719]

> By the same token that evidence derived from the use of torture must always be rejected so as to safeguard the integrity of the judicial process and avoid bringing British justice into disrepute …, so too in my judgment must closed material be rejected if reliance on it would necessarily result in a fundamentally unfair hearing.

386. The IPT model is, therefore, an inadequate answer to the question first raised by the judgment of the ECtHR in *Klass*: how do you devise a fair procedure to deal with complaints concerning secret surveillance without disclosing whether or not surveillance has taken place? The grossly unfair nature of the Tribunal's procedures is undeniably a serious problem and no doubt has led to some potentially meritorious complaints being dismissed because of the inherently one-sided nature of its scrutiny. But the broader problem is that, even if the Tribunal somehow managed to adopt a procedure that was entirely fair, the secret nature of surveillance powers would still mean that it would continue to receive a large number of complaints from people whose suspicions proved to be groundless, while most of those people who were the subject of genuinely unnecessary surveillance would remain quietly oblivious to that fact.

387. There are, therefore, a number of steps that need to be taken to make the Tribunal an effective mechanism against unnecessary and disproportionate surveillance.

388. First, as we have noted throughout this report, increasing the use of prior judicial authorisation would dramatically reduce the need for the Tribunal in the first place, by ensuring that decisions concerning more intrusive forms of surveillance by police and the intelligence services, or any surveillance decision by another public body, would be made by a judge rather than a member of the executive. The role of the tribunal in such cases would necessarily be more limited, ie, reviewing whether the judge's decision was correct in law and determining whether the surveillance carried out by the public body did not exceed the terms of the warrant or authorisation. Even allowing for a significant increase in the use of prior judicial authorisation, however, there would still be a role for the Tribunal concerning the use of less intrusive forms of surveillance, eg, directed surveillance by police, in which the first instance decision would not be made by a judge. The Tribunal would also continue to have an important role to play in investigating claims of any unauthorised surveillance by public bodies.

389. Second, although the ECtHR in *Klass* dismissed the use of mandatory ex post facto notification requirements, these remain a well-established feature of the surveillance laws of other countries, including the United States, Canada, Germany, Denmark and the Netherlands. In our view, the experience of other countries shows that similar requirements would be a proportionate restriction on the need to maintain operational secrecy. In particular, we endorse the recommendation of the House of Lords Constitution Committee that 'individuals who have been made the subject of surveillance be informed of that surveillance, when completed, *where no investigation might be prejudiced as a result*'.[720]

---

718. *R(Secretary of State for the Home Department v Assistant Deputy Coroner for West London* [2010] EWC 3098 at para 24.
719. [2007] UKHL 46 at para 91.
720. See n72 above, para 163. Emphasis added.

390. Third, given the obvious shortcomings of the reactive nature of the Tribunal, it is also important to increase significantly the number of routes by which the investigative functions of the Tribunal may be brought into play. We have already seen in relation to the Code of Practice governing encryption key notices, for instance, that the relevant oversight commissioners are obliged to notify any individuals adversely affected by a 'wilful or reckless failure' of a public authority of the exercise of its powers under Part 3 of RIPA. We see no reason, however, why the relevant oversight commissioner should not be obliged to refer cases *directly* to the Tribunal, and in cases not just limited to the use of encryption keys, or the relatively high threshold of 'wilful or reckless failure' by a public authority. Other public bodies with relevant oversight functions, such as the Independent Police Complaints Commission or the Metropolitan Police Authority for instance, could also be given the power to refer cases to the Tribunal where appropriate.

391. Fourth, the Tribunal itself must become more proactive in its investigations and work more closely in conjunction with the inspection regimes of the relevant oversight commissioner to investigate surveillance decisions in circumstances where problems are known to exist, eg, the well-documented failings of the Prison Service. In particular, the Tribunal must demonstrate that it has the necessary wherewithal to investigate claims of unauthorised surveillance in circumstances where there are good reasons to suspect that the public body in question may be less than fully cooperative.

392. Fifth, in the absence of anything approaching equality of arms between the parties before the Tribunal, the Tribunal itself needs to develop *internal* procedures that introduce a greater degree of adversarial testing of the government's case. As we set out in Part 4 of our report, *Secret Evidence*, there are a number of mechanisms that have been developed in various jurisdictions including our own to enable a degree of internal adversarial challenge without disclosure of the case to the complainant. These have included the use of special advocates before the Canadian Security and Intelligence Review Committee (the inspiration for special advocates in the UK), the role of the public interest advocate in Queensland; and even the use of special advocates in Public Interest Immunity applications in the UK (see eg, the *Binyam Mohamed* case before the Divisional Court). One of the failings of the Strasbourg Court's analysis in *Kennedy* was that it accepted at face value the government's claim that:[721]

> unless they were appointed in every case, the appointment of special advocates would also allow a complainant to draw inferences about whether his communications had been intercepted.

There are at least two flaws with this reasoning. The first is that a complainant obviously does not need to be told if a special advocate has been appointed. Although it is important in the context of closed proceedings in general for a special advocate to consult a complainant and to take what instructions she can, the reality of the special advocate's task is that communication with the complainant is unlikely to be necessary in order to adversarially test the material in question at the initial sifting stage. Indeed, as the Queensland and Canadian examples show, not all procedures for internal adversarial testing require the special advocate to actually represent the interests of a complainant. In more inquisitorial proceedings, it may often be just as effective to task the special advocate with representing the public interest in ensuring that surveillance powers are not misused

721. *Kennedy*, para 182. See para 187: The Court agrees with the Government that, in the circumstances, it was not possible to disclose redacted documents or to appoint special advocates as these measures would not have achieved the aim of preserving the secrecy of whether any interception had taken place'.

or abused. As we suggest below, it may only be once a complaint has reached a certain stage, ie, an inter partes hearing, that communication with the complainant becomes important. The second flaw in the Court's reasoning is, of course, that there is no reason apart from cost why special advocates should not be appointed in every case. No doubt this would be more expensive, but – as we noted in our 2009 report – this is ultimately the price of having fair proceedings.

393. Sixth and last, if the Tribunal is to have any hope of resembling a court with fair procedures, then there needs to be some relaxation of the 'neither confirm nor deny' policy (NCND). It is, of course, apparent from cases such as *Klass* onwards that the need to preserve NCND has been treated as axiomatic to any legal framework governing the use of surveillance powers. It is not entirely clear, however, why this should be the case. Indeed, it is somewhat disturbing that the courts have been so willing to accommodate NCND even at the cost of considerable damage to the principles of open justice and procedural fairness and ultimately their own integrity. Certainly, respect for NCND and the effectiveness of surveillance in general are in the public interest, but so too are things like procedural fairness and effective protection for the right to privacy. It is, therefore, no answer to say that NCND must be preserved at all costs. After all, NCND is already subject to the obvious exception that a complainant may be notified of a successful complaint, even though this would undoubtedly be helpful to others who may wish to evade similar surveillance. The revelation that Poole Borough Council was authorising its officers to use a Canon EOS300D Digital Camera to conduct covert surveillance of the Paton family,[722] for instance, was undoubtedly in the public interest but it also gave a clearer indication of some of its surveillance methods, information that might also have assisted the fly-tippers of Dorset for a time. As the Court of Appeal held in the *Binyam Mohamed* case, the public interest in the fair administration of justice is sometimes sufficient to outweigh the corresponding public interest in ensuring that foreign intelligence material is not disclosed in breach of undertakings given by our intelligence services. If even the so-called 'control principle' is not absolute in a case involving material passed by the CIA, then it is difficult to see why NCND should be.

394. More to the point, some relaxation of NCND is unlikely to involve the end of secret surveillance as we know it. There are, after all, degrees of secrecy. It may be the case that NCND remains the default position at the initial stage, similar to permission stage in judicial review proceedings, but that there is an entitlement to limited disclosure in any case that reaches a certain threshold, eg, where the Tribunal is satisfied that there is a serious issue to be determined and that the public interest in the fair administration of justice outweighs that in the continuing secrecy of a surveillance operation. In the same way that we doubt that merely publishing the numbers of interception warrants signed by the Foreign Secretary provides much of an indication to hostile forces as to the true extent of MI6's interception capabilities, we similarly doubt that relaxing the NCND requirement in this way would significantly impair the general surveillance capabilities of the police, intelligence services and other public authorities.

722. *Paton v Poole Borough Council*, n42 above, para 21.

Recommendations

Increase the use of prior judicial authorisation for surveillance decisions in general

395. Increasing the use of prior judicial authorisation would significantly reduce the pressure on the Tribunal to provide an effective check against unnecessary or disproportionate cases. This would also have the benefit of freeing up the Tribunal's resources to investigate complaints concerning: i) the use of less intrusive forms of surveillance by the police and intelligence services; and ii) the unauthorised use of surveillance by any public body.

Introduce mandatory notification requirements following the completion of surveillance

396. In other countries, mandatory notification requirements are a well-established mechanism in allowing people who have been the subject of surveillance to bring a complaint before the Tribunal. We endorse the recommendation of the House of Lords Constitution Committee that 'individuals who have been made the subject of surveillance be informed of that surveillance, when completed, where no investigation might be prejudiced as a result'.[723]

Increase the number of routes by which the Tribunal may be notified of a case

397. In line with our recommendations in previous chapters, the relevant oversight commissioner should be required to refer cases to the Tribunal for investigation whenever he or she reasonably suspects that a public authority has breached the requirements of RIPA, including the unnecessary or disproportionate use of surveillance powers. Similarly, other relevant oversight bodies (eg, the Independent Police Complaints Commission) should also have the power to refer cases to the Tribunal in similar circumstances.

Increase the capabilities of the Tribunal to enable it to undertake proactive investigations

398. The inspection regimes of the relevant oversight commissioner should be more closely linked to the Tribunal to enable it to investigate possible complaints arising from systemic failings, eg, the use of interceptions by the Prison Service. The Tribunal must also have sufficient resources to investigate claims of unauthorised surveillance beyond that provided by the cooperation of the relevant public body.

Adopt internal measures to increase adversarial testing of relevant evidence

399. The Tribunal should appoint a panel of special advocates to act in any case where its investigations have identified a case to be answered. This would not require notice to the person affected in the first instance, but would enable the public body's case to be subject to internal adversarial testing. This recommendation is consistent with those made in our 2009 report *Secret Evidence*, and resembles, in particular, the work of the Queensland Public Interest Monitor in surveillance cases.[724]

---

723. N72 above, para 163.
724. See pp 177-179 of *Secret Evidence* (JUSTICE, 2009).

Relax the existing policy of NCND sufficient to enable the Tribunal to adopt fair procedures

400. The Tribunal's respect for the general policy of NCND whether surveillance has taken place must be relaxed. NCND should remain the default position at the initial stage of investigating complaints, but should be departed from in any case where the Tribunal is satisfied that there is a serious issue to be determined and that the public interest in the fair administration of justice outweighs that in the continuing secrecy of a surveillance operation.

Chapter 10
Conclusion

Surveillance reform for a digital age

401. At the launch of his company's new networking software in January 1999, Scott McNealy, the CEO of Sun Microsystems, was speaking to reporters and analysts about Internet security.[725] Dismissing concerns about online consumer privacy as a 'red herring', he apparently told the group, 'You have zero privacy anyway. Get over it'. Over a decade later, Mark Zuckerberg, the CEO of Facebook, told an audience in San Francisco:[726]

> When I got started in my dorm room at Harvard, the question a lot of people asked was 'why would I want to put any information on the Internet at all? Why would I want to have a website?' And then in the last 5 or 6 years, blogging has taken off in a huge way and all these different services that have people sharing all this information. People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.

Whether or not a billionaire with a financial interest in harnessing his customers' private information is really the most objective person to assess a change in social norms, it seems clear that the digital capabilities of modern technology have begun to outstrip and erode our traditional expectations of privacy. But, contrary to the claims of some CEOs, this loss of privacy is not something to be accepted but something to be resisted and reversed. And central to this is a robust legal framework for its protection.

402. The law governing privacy is, of course, an issue that extends well beyond the use of surveillance by public bodies. But, as we have seen from the recent phone hacking saga, the legal framework for the use of surveillance powers lies at the heart of the broader law protecting privacy in the UK. It is, therefore, important to get that framework right. This is not just because privacy is important but because surveillance is important. It is, after all, a necessary activity in the fight against serious crime and a vital part of our national security. It has saved countless lives and helped convict hundreds of thousands of criminals.

---

725. 'Sun on Privacy: 'Get Over It'', by Polly Sprenger, *Wired,* 26 January 1999.
726. 'Privacy no longer a social norm, says Facebook founder', the *Guardian,* 11 January 2010.

403. Unnecessary and excessive surveillance, however, destroys our privacy and blights our freedoms. As Sir Erskine May wrote in the mid-19th century, 'the freedom of this country may be measured by its immunity' from what he described as the 'baleful agency' of the kinds of 'espionage which forms part of the administrative system of continental despotisms'. If that were true, however, then the freedom of this country is in a very sorry state indeed. Because RIPA has not only failed to check a great deal of plainly excessive surveillance by public bodies over the last decade but also, in many cases, inadvertently encouraged it. Its poor drafting has allowed councils to snoop, phone hacking to flourish, privileged conversations to be illegally recorded, and CCTV to spread.

404. After all, the importance of clear, well-drafted legislation is not just that it helps to meet the foreseeability requirements of Article 8(2) of the ECHR but also that it is easier for people to follow and courts to apply. RIPA, by contrast, is poorly drafted and hopelessly lacking in clarity. As the President of the IPT Lord Justice Mummery himself conceded in 2006:[727] 'The experience of the tribunal over the last five years has been that RIPA is a complex and difficult piece of legislation'. A degree of complexity is perhaps inevitable when dealing with an issue as complex as surveillance. Nonetheless the need for legislation to be as simple and as clear as possible was powerfully expressed by Baroness Hale in a lecture earlier this year:[728]

> [T]he law – the content of it – needs to be accessible. To be accessible it ought to be clear and simple. This seems to be a vain hope in today's complicated society … A great deal of time, trouble and money is wasted when the law is complex and unclear. It is a mistake to think that most lawyers want the law to be complex and unclear. There may be some top advocates in the higher courts who relish the wriggle room that unclear law gives them. But surely most want to be able to give their clients clear advice. Their clients' lives are messy enough. *The law should not also be a mess.*

RIPA is not only unclear in its language but also very poorly thought out; especially its inadequate definitions of surveillance, its provision of no less than three oversight commissioners and four different schemes for authorisation.

405. RIPA is also badly out of date. As we noted in our report 40 years ago, the traditional protections of the common law against eavesdroppers and peeping toms were already inadequate at the beginning of the 1970s, at a time when the average computer was still the size of a refrigerator and Britain's streets were free of CCTV. Despite the fact that RIPA was enacted in 2000, at a time when the digital revolution was already well underway, it is plain that it is equally inadequate to cope with such developments as aerial surveillance drones, Automatic Number Plate Recognition, deep packet interception, and, indeed, the Internet itself.

406. Most of all, for the reasons set out in this report, RIPA fails to provide adequate safeguards against unnecessary and disproportionate surveillance. Indeed, with the honourable exception of the work of the Surveillance Commissioners in authorising intrusive surveillance, RIPA offers something worse: an illusion that the law is compatible with fundamental rights, one that conceals the reality of widespread executive self-authorisation, limited oversight, and only the most remote prospect of any kind of redress.

---

727. *C v the Police and Secretary of State for the Home Department* (IPT/03/32/H, 14 November 2006), para 22.
728. Equal Access to Justice in the Big Society', Sir Henry Hodge Memorial Lecture 2011, p3.

407. Although the amendments put forward by the Protection of Freedoms Bill are welcome, they are nowhere near enough: they are piecemeal amendments and RIPA is already a piecemeal Act. Root-and-branch reform of the law on surveillance is needed to provide freedom from unreasonable suspicion, and put in place genuinely effective safeguards against the abuse of what are necessary powers. In particular, our recommendations summarised below follow a number of general principles that we have identified in the course of this report. These are:

i. *Prior judicial authorisation for surveillance decisions* is the best safeguard against unnecessary and disproportionate interference with individual privacy. No matter how conscientious or diligent senior police officers, intelligence officials, civil servants or government ministers may be, they lack the necessary independence from the executive to provide an effective safeguard. This is, of course, why English judges have been responsible for the making of search warrants for centuries: it reflects the importance that we attach to respect for private property by requiring the executive to make its case before an independent and impartial judge.[729] This is what the ECtHR has consistently recognised in its case law, beginning with *Klass.* It is also, not incidentally, why the Surveillance Commissioners – who are all serving or retired judges – are responsible for authorising the use of intrusive surveillance by the police under Part 2 of RIPA. We have not recommended that surveillance warrants issued by a judge are necessary in *all* cases: in particular, there is a great deal of relatively 'low level' surveillance that is carried out by the police and the intelligence services that would be both unnecessary and impractical to seek judicial authorisation for: eg, following a suspect's movements in public over the period of a week. Rather, we recommend that the need for prior judicial authorisation should reflect two factors: i) the intrusiveness of the surveillance (which should *not* be confused with the relatively narrow definition of 'intrusive surveillance' under Part 2 of RIPA); and ii) the nature of the agency responsible for carrying out the surveillance. In our view, the police, law enforcement bodies, and intelligence services can generally be trusted to use low-level surveillance in their day-to-day work without seeking the authorisation of a judge. It is not appropriate for non-law enforcement bodies, eg, local councils or the NHS Care Standards Commission, to use even low-level surveillance powers without judicial supervision. By contrast, use of intrusive surveillance methods (including interceptions) must always be authorised by a judge, no matter how experienced the agency carrying out the surveillance. It is possible to have a system of self-authorisation in an emergency (as, indeed, Part 2 of RIPA provides even in the case of intrusive surveillance by police). More generally, as Annex A makes clear, prior judicial authorisation of surveillance is standard practice in every other European and common law jurisdiction. It is, therefore, impossible to see why it should not also be standard practice in the UK.

ii. *Ex post facto oversight of surveillance powers by commissioners is, by contrast, of very limited effectiveness and must be rationalised.* One of the striking features of RIPA is the number of overlapping oversight commissioners: the Interception of Communications Commissioner (who has responsibility over interceptions but also communications data requests and some

729. See also eg, the recent comments of the Lord Chief Justice Lord Judge on the value of independent judicial decisions at the Lord Mayor's Dinner for HM Judges, Mansion House, 13 July 2011: 'the country is in the middle of the crisis that has embroiled the press and the politicians and the police. Perhaps it is just worth noticing that there would not have been any crisis but for public revulsion at the breaches of the confidentiality involving the victims of crime and war. And now, notwithstanding the constant criticism of judges public revulsion has led to the public demand for a judge led inquiry. That is not because anyone assumes that judges are infallible, or that the conclusions of judges will always carry universal acclaim. It is rather because the public knows that judges are men and women of independent mind, who can be relied to draw whatever conclusion from the evidence seems right and who, notwithstanding whatever pressures there may be, can be relied on to deliver a carefully considered, honest, but above all, an independent answer. The public understands that we are indeed independent. Not infallible certainly, but independent, always. It is a cherished quality'.

oversight of encryption notices); the Intelligence Services Commissioner (who oversees the use of surveillance under RIPA by the intelligence services under Parts 2 and 3, with the exception of interception under Part 1); and the Chief Surveillance Commissioner (who oversees the use of surveillance under Parts 2 and 3 of RIPA by the police, other law enforcement bodies and all other public bodies except the intelligence services). To this, the Protection of Freedoms Bill proposes to add a Surveillance Camera Commissioner. In addition, there is an important parallel oversight role played by the Information Commissioner in relation to data protection and other privacy concerns. This is, plainly speaking, a hopeless arrangement, involving the unnecessary proliferation of entities. The second striking feature of the oversight arrangements under RIPA is how limited they are. Their most important function appears to be the provision of inspection regimes of the various agencies carrying out surveillance. However, the actual review of surveillance decisions appears to be extremely limited: the selection of a dip sample of authorisations or warrants whose size remains unknown but – as far as anyone can tell – may be less than five per cent. More generally, several of the commissioners have produced reports that have varied little in their content from year to year. It is ironic that in 2005, the Chief Surveillance Commissioner (whose own reports are a fortunate exception to this rule) criticised the quality of authorisations for directed surveillance made by public bodies, saying that they 'must be intelligently completed without recourse to cut-and-paste'.[730] It is a criticism that could equally be applied to the reports of the Intelligence Services Commissioner or the Interception of Communications Commissioner. More generally, it makes little sense to have the same activity (eg, the making of encryption key notices) subject to oversight by as many as three different commissioners, depending on the agency involved. We, therefore, recommend that the oversight regime be rationalised, with the Office of the Chief Surveillance Commissioner assuming responsibility for oversight of the overwhelming majority of surveillance activities, including interception and all surveillance carried out by the intelligence services within the jurisdiction of the UK. We also recommend that the supervisory role of the Information Commissioner, who has substantial experience of privacy issues in relation to his oversight role over data protection, be extended to include so-called business interceptions and 'unintentional' interceptions by communications service providers, as well as communications data requests by non-law enforcement bodies. This is because of the now-substantial overlap between data protection issues and the privacy concerns raised by digital communications that do not involve the investigation of serious crime and/or threats to national security.

iii. *An IPT that relies solely on complaints brought by members of the public based on their suspicions alone can never be an effective check against unnecessary or disproportionate surveillance decisions.* As Lord Neuberger noted in *In Re McE* in 2009, the use of secret surveillance involves at least two inherent paradoxes. The first is that it involves an inevitable degree of self-justification in that the basis for invading someone's privacy is the suspicion that they are involved in some kind of wrongdoing, which suspicion cannot be verified without invading their privacy. The second paradox, highlighted in *Klass*, is that the most effective safeguard against the unnecessary invasion of a person's privacy by a public body – ie, giving that person prior notice and allowing them the opportunity to argue their case before an independent judge – is impossible because it would defeat the very purpose of the surveillance. In almost every case, therefore, victims of the misuse or abuse of surveillance powers will never know their privacy has been unjustifiably violated. As the sorry record of the Tribunal over the past

730. *Annual Report of the Chief Surveillance Commissioner 2004-2005* (HC 444, November 2005), para 8.10.

decade shows – about three million surveillance decisions, over a thousand complaints but only ten upheld, five of which came from the same case – a mechanism that relies solely on members of the public bringing complaints based on their suspicion can never be an effective check against the abuse of surveillance powers.

iv. *The law on surveillance must be made as clear and transparent as possible.* As we have already seen, poor drafting and unnecessary complexity gives rise to a host of problems: the law is uncertain, difficult for public servants to follow, and difficult for courts and tribunals to apply; it gives rise to an increased risk of errors and, worse, the possibility of loopholes being exploited: something which, in turn, is enormously difficult to detect given the secret nature of surveillance itself. We do not know, for instance, if the narrow definition of section 1 of RIPA adopted by the Metropolitan Police was used in other circumstances by the police or indeed other public authorities to sanction the interception of communications without a warrant. This, in turn, reduces the possibility of effective democratic oversight of the law on surveillance, something which is essential if the public are to meaningfully debate whether to change the law, and what changes should be made. For better or for worse, surveillance will always be a technical and complex area of the law, but that is surely no reason to make it any more technical and more complex than it needs to be.

Summary of recommendations

Chapter 3: Interception of communications

1. Introduce prior judicial authorisation for interception warrants (**paras 141-143**);

2. Transfer responsibility for oversight of interception warrants to the Chief Surveillance Commissioner and responsibility for oversight of so-called 'unintentional' interceptions by businesses and communications service providers to the Information Commissioner (**para 144-146**);

3. Improve the clarity and flexibility of the law relating to interception (**para 147**);

4. Lift the ban on the use of intercept material as evidence in criminal and civil proceedings (**para 148**);

Chapter 4: Communications data

5. Introduce and extend the use of prior judicial authorisation for requests for communications data as proposed by the Protection of Freedoms Bill to all public bodies, with the exception of requests for subscriber data by the police, other law enforcement agencies, the intelligence services and the emergency services (**paras 190-193**);

6. Reduce the number of public bodies with access to communications data (**paras 194-195**);

7. Transfer responsibility for oversight of communications data requests to the Chief Surveillance Commissioner (concerning requests for data by the police, the intelligence services, and other national law enforcement bodies) and the Information Commissioner (requests for data by all other, non-law enforcement bodies such as local authorities, fire and ambulance services) (**paras 196-199**);

Chapter 5: Intrusive surveillance

8. Establish a single warrant for intrusive surveillance and property interference ('surveillance warrants') (**para 243**);

9. Broaden the definition of 'intrusive' surveillance to cover *all* surveillance likely to constitute a serious interference with a person's privacy under Article 8, eg, *any* surveillance of privileged communications, confidential personal information or confidential journalistic information (**para 244**);

10. Require all surveillance warrants to be made by a judge (**para 245-246**);

11. Transfer responsibility for oversight of the use of intrusive surveillance in the UK from the Intelligence Services Commissioner to the Chief Surveillance Commissioner (**para 247**);

Chapter 6: Directed surveillance

12. Revise the definition of 'directed surveillance' to cover any covert surveillance that seeks to obtain information about an individual but does not otherwise involve significant interference with their privacy; as well as any use of overt surveillance, including CCTV or ANPR, in a targeted manner for the purposes of a specific investigation or the surveillance of a particular person (**paras 283-284**);

13. Extend prior judicial authorisation for the use of directed surveillance as proposed by the Protection of Freedoms Bill to *all* public bodies *except* the police, intelligence services and other law enforcement agencies with responsibility for investigating and prosecuting serious crime, and for whom the purpose of surveillance is obtaining admissible evidence (**paras 285-286**);

14. Transfer responsibility for oversight of the use of directed surveillance by the intelligence services within the UK from the Intelligence Services Commissioner to the Chief Surveillance Commissioner (**para 287**);

15. Adopt a mandatory Code of Practice for surveillance cameras that applies to both public and private bodies, and involves both criminal and civil sanctions (**para 288**);

16. The proposal in the Protection of Freedoms Bill for a Surveillance Camera Commissioner to supervise the mandatory Code of Practice should be abandoned. Instead, the Information Commissioner's Office should have primary responsibility for regulation of surveillance cameras, with the assistance of the Chief Surveillance Commissioner in respect of any surveillance system regularly used for the investigation of serious crime (**para 288**);

Chapter 7: Covert human intelligence sources

17. Extend prior judicial authorisation for the use of covert sources as proposed by the Protection of Freedoms Bill to *all* public bodies *except* the police, intelligence services and other law enforcement agencies (**para 307**);

18. Complex operations involving the use of undercover officers should be subject to authorisation by warrant issued by a Surveillance Commissioner (**para 306**);

19. Transfer responsibility for oversight of the use of covert sources by the intelligence services within the UK from the Intelligence Services Commissioner to the Chief Surveillance Commissioner (**para 307**);

Chapter 8: Encryption keys

20. Extend the safeguard of prior judicial authorisation for all encryption key notices, including those involving encrypted interceptions, communications data and the intelligence services (**paras 343-344**);

21. In cases where a person is required by an encryption notice to provide the key to, or otherwise decrypt, his own material, any application should be made inter partes to allow him to challenge the public authority's decision at the permission stage (**para 345**);

22. Transfer responsibility for oversight of the use of encryption key notices from the Interception Commissioner and the Intelligence Services Commissioner to the Chief Surveillance Commissioner (**paras 346-347**);

Chapter 9: The Investigatory Powers Tribunal

23. Increase the use of prior judicial authorisation for surveillance decisions in general (**para 395**);

24. The relevant oversight commissioner should be required to refer cases to the Tribunal for investigation whenever he or she reasonably suspects that a public authority has breached the requirements of RIPA, including the unnecessary or disproportionate use of surveillance powers. Other relevant oversight bodies (eg, the Independent Police Complaints Commission) should also have the power to refer cases to the Tribunal in appropriate cases (**para 397**);

25. Within a reasonable period following the conclusion of a surveillance operation, the subjects of that surveillance should be notified and provided with sufficient details of the surveillance undertaken to enable them to bring a complaint to the Tribunal, where the oversight Commissioner is satisfied that to do so would not compromise any ongoing investigation (**para 396**);

26. The investigative capabilities of the Tribunal should be increased and extended to enable it to undertake proactive investigations arising from any systemic failings identified by the relevant oversight commissioner, or in cases in which there are reasonable grounds to suspect the unauthorised use of surveillance by a public body (**para 398**);

27. The Tribunal should adopt *internal procedures to increase adversarial testing of relevant evidence, including the appointment of a standing panel* of special advocates to act in any case where its investigations have identified a case to be answered (**para 399**); and

28. The existing policy of neither confirming nor denying the existence of surveillance should be relaxed sufficiently to enable the Tribunal to adopt fair procedures (including the right to an oral hearing, disclosure of evidence, cross examination of witnesses, and the giving of reasons) in any case where the Tribunal is satisfied that there is a serious issue to be determined and that the public interest in the fair administration of justice outweighs that in the continuing secrecy of a surveillance operation (**para 400**).

Annex

Comparative use of judicial authorisation for surveillance powers in other European and common law countries

	Interception of Communications	Communications Data	Intrusive Surveillance	Directed Surveillance	Covert Sources
Australia[a]	Yes	No	Yes	No	No
Canada[b]	Yes	No	Yes	No	No
France[c]	Yes	No	Yes	No	Yes
Germany[d]	Yes	Yes	Yes	No	Yes
Ireland[e]	No	No	Yes	No	No
New Zealand[f]	Yes	No	Yes	No	No
Spain[g]	Yes	Yes	Yes	No	Yes
South Africa[h]	Yes	Yes	Yes	No	No
Sweden[i]	Yes	Yes	Yes	No	No
US[j]	Yes	Yes	Yes	No	No
UK[k]	No	No	Yes[l]	No	No

a See the Telecommunications (Interception and Access) Act 1979; the Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011; the Surveillance Devices Act; and the Australian Security Intelligence Organisation Act 1979.

b See the Criminal Code; the Canadian Secret Intelligence Service Act; and the Personal Information Protection and Electronic Documents Act 2004.

c Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques; Code de procédure pénale.

d Act Reforming Telecommunications Surveillance and Other Covert Investigative Measures and Transposing Directive 2006/24/EC; Code of Criminal Procedure; Telecommunications Data Protection Ordinance.

e See the Criminal Justice (Surveillance) Act 2009; the Communications (Retention of Data) Act 2011; and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

f See the Crimes Act 1961, the Misuse of Drugs Amendment Act 1978, the New Zealand Security Intelligence Service Act 1969, the Government Communications Bureau Act 2003 and the Video Camera Surveillance (Temporary Measures) Bill introduced following the decision of the NZ Supreme Court in Hamed and others v The Queen [2011] NZSC 101.

g Ley de Enjuiciamiento Criminal; Ley de Protección de Datos.

h Regulation of Interception of Communications Act 2003.

i Ch 27 of the Code of Judicial Procedure.

j Title III of the Omnibus Crime Control and Safe Streets Act 1968 (US Code, Title 18, Chapter 119) and the Foreign Intelligence Surveillance Act 1978.

k RIPA.

l Except for the use of intrusive surveillance by the intelligence services.

In 2000, Parliament enacted the Regulation of Investigatory Powers Act (RIPA) 2000. At the time, it was acclaimed by government ministers as human rights-compliant, forward-looking legislation. Since its inception, there have been close to three million decisions taken by public bodies under RIPA.

Surveillance is a necessary activity in the fight against serious crime. It is a vital part of our national security. It has saved countless lives and helped convict hundreds of thousands of criminals. Unnecessary and excessive surveillance, however, destroys our privacy and blights our freedoms.

RIPA has not only failed to check a great deal of plainly excessive surveillance by public bodies over the last decade but, in many cases, inadvertently encouraged it. RIPA is neither forward-looking nor human rights compliant. Piecemeal amendments are no longer enough for what is already a piecemeal Act.

JUSTICE's report, *Freedom from Suspicion, Surveillance Reform for a Digital Age*, responds to these issues, covering:

- Surveillance and the right to privacy
- Interception of communications
- Communications data
- 'Intrusive' Surveillance
- 'Directed' Surveillance
- Covert human intelligence sources
- Encryption keys
- The Investigatory Powers Tribunal

Root-and-branch reform of the law on surveillance is needed to provide freedom from unreasonable suspicion, and put in place truly effective safeguards against the abuse of what are necessary powers. This report outlines a series of recommendations to serve as the basis for a draft Surveillance Reform Bill.

THE JOSEPH ROWNTREE CHARITABLE TRUST

JUSTICE would like to thank the Joseph Rowntree Charitable Trust for its funding of this project.

£10.00

ISBN 978-0-907247-53-1