The Information Commissioner's submission to the Royal United Services Institute's Independent Surveillance Review Panel

Summary

- Effective oversight and redress is an essential component in inspiring and maintaining public trust and confidence
- The current legal and regulatory regime is fragmented and needs review to ensure that it is fit for purpose in providing appropriate and effective oversight and redress mechanisms, given the rapid developments in digital technology in use today and likely to be in use in the foreseeable future
- There is a need to introduce greater transparency and accountability
- A 'privacy by design' approach should be adopted to utilise the power of technology to minimise privacy intrusion
- Ethical consideration needs to be given to any surveillance or interception activities even when there is a lawful basis

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), together with associated legislation such as the Privacy and Electronic Communications (EC Directive) Regulations 2003(PECR). The Information Commissioner also has some oversight in relation to the Data Retention Regulations 2014 as he will be required to audit compliance with requirements and restrictions in relation to the 'integrity, security or destruction' of the data being retained by Communication Service Providers (CSPs).

2. He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals and taking appropriate action where the law is broken.

3. The Panel's Inquiry is focussed on the current and future requirements for digital information for public authorities, the privacy implications of the UK Government's current interception capabilities, the privacy safeguards needed in an era of big data, the suitability of the UK's current statutory oversight arrangements

in relation to the retention and use of data, and the challenges faced by the UK Government in providing security and privacy for its citizens in an era rapidly evolving communications technology.

Background

4. The Information Commissioner and his predecessors have been concerned about the increasing surveillance of UK citizens in many different contexts and clearly the Snowden disclosures have again heightened concerns in this area. A report on 'the surveillance society' was commissioned in 2006 and this led to inquiries by two Parliamentary committees to which the Information Commissioner gave evidence. The Home Affairs Committee in its report on its Inquiry entitled 'A Surveillance Society' (HC 58-1) recommended that the Information Commissioner produce a further report to Parliament on the state of surveillance (recommendation 2, paragraph 36). This further report was provided to the Committee in 2010 updating the earlier report and highlighting the Information Commissioner's view on key regulatory and other responses that could usefully be adopted.

5. The Information commissioner recognises that decisions on the extent of surveillance that are considered necessary and proportionate in the UK are ultimately for ministers and Parliament rather than for him. The Commissioner's primary role is in ensuring that there are suitable safeguards for privacy in place and in contributing to effective regulatory oversight. In this context he recommended to the Home Affairs Committee that there are a number of key areas that need to be addressed to help ensure a proper balance between the privacy of the individual and the wider interests of society. These recommendations focussed on increasing accountability and transparency in the adoption and use of potentially intrusive surveillance related legislative measures. Those recommendations are of particular relevance to concerns about the propriety and effectiveness of the current legal framework and included:

- Increased adoption of 'privacy by design' approaches to minimise intrusion
- A requirement for a privacy impact assessment[1] to be presented during the Parliamentary process where legislative measures have a particular impact on privacy
- An opportunity for the Information Commissioner to provide a reasoned opinion to Parliament on measures that engage concerns within his areas of competence

[1] The Information Commissioner has developed a code of practice on conducting privacy impact assessments https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

- Increased post legislative scrutiny of legislation, based on a formal report on the deployment of the legislation in practice, the value of the information collected, the impact on privacy and the continued need for such measures
- In certain appropriate circumstances inclusion of a sunset clause in legislation that is particularly privacy intrusive

Privacy Impact

6. Any intrusion into the privacy of citizens, whether this be by way of Closed Circuit Television (CCTV), Automatic Number Plate Recognition (ANPR) cameras, Unmanned Aerial Vehicles (commonly known as drones) or monitoring communications and other internet use such as social networking, will engage fundamental human rights concerns. It will need to comply with the DPA, Article 8 of the European Convention of Human Rights and, of increasing significance, Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Any processing of personal data, including the collection of data and access to stored data, needs to be necessary, proportionate and justified with effective oversight arrangements in place. It is important to bear in mind here that even just the collection of personal data is an intrusion, not least because once collected the data are vulnerable to misuse or loss. It is not the case, as some argue, that intrusion only takes place when the collected data start to be used.

7. Whatever the level of intrusion, privacy safeguards should always be considered. The extent of these safeguards will depend upon the nature of the surveillance activity concerned. Transparency is important; but, for example, public space CCTV surveillance is largely conducted in an overt manner with signs alerting individuals to its presence so a degree of transparency is effectively built into the system. Whilst advanced facial recognition systems are available, the identification of an individual within CCTV data is a task of much greater computational difficulty than searching for an IP address, keyword, or other unique identifier in a repository of communications data. Identification errors are likely, so safeguards are needed to keep errors to a minimum and ensure that they do not cause prejudice to individuals. Retracing the daily movements of a specific individual from mobile phone records is a far easier option than searching through CCTV data but it needs to be remembered that subscribers may not always be in possession of their own mobile phones.

8. Furthermore, interception of an individual's communication or communications data can be achieved so covertly that it can be without the knowledge of the individual or even the

communications provider. The state surveillance of individuals' communications, be this content or metadata, engages significant privacy and data protection concerns. The DPA provides only limited reassurance as a wide ranging exemption from its provisions can be relied on where safeguarding national security is engaged (Section 28 of the DPA).

9. Metadata itself can be very revealing and intrusive in a wide range of contexts. It can provide not just the details of who is calling who but also location information, frequency of contact, for how long the contact takes place and other patterns of behaviour. Indeed, modern communications equipment is continually connected to a network and constantly transmitting and receiving data without involvement of the individual, leading to an almost constant stream of metadata. The Information and Privacy Commissioner for Ontario has published a report[2] highlighting the potentially intrusive nature of metadata. The Article 29 Working Party has also recently recognised that the analysis of metadata may reveal sensitive data about individuals.[3]

Encryption

10. A recent media story (Guardian, 6 February 2015) 'Security Services Capable of Bypassing Encryption, Draft Code Reveals' [4] highlights that Britain's security services have acknowledged that they have the worldwide capability to bypass the use of encryption by internet companies by attacking the computers of end users directly.

11. The Information Commissioner is concerned about this and, as disclosed in the Snowden revelations, the exploitation of encryption and other software vulnerabilities by the security services, in order to intercept communications and access communications data. The use of encryption is necessary to provide protection against unauthorised access to personal data. Many breaches of personal data reported to the Information Commissioner could have been prevented, or risks resulting from a breach minimised, if the data controller had adequately addressed vulnerabilities in their information systems or applied effective encryption techniques.

---

[2] A Primer on Metadata: Separating Fact from Fiction
http://www.privacybydesign.ca/content/uploads/2013/07/Metadata.pdf

[3] Pp 4-5. Article 29 Working Party Opinion 04/2014 (WP215) on surveillance of electronic communications for intelligence and national security purposes – 10 April 2014

[4] http://www.theguardian.com/uk-news/2015/feb/06/uk-security-services-capable-bypassing-encryption-draft-code

12. Allegations that the security services have required commercial providers deliberately to introduce vulnerabilities or to intentionally choose default systems which provide an ineffective standard of protection are extremely concerning. Of similar concern are allegations that the security services are actively and covertly collecting knowledge of previously unknown vulnerabilities so that these can be used to intercept communications in the future. The knowledge and non-disclosure of such vulnerabilities leaves the door open for other parties with malicious intent to attack and penetrate systems putting personal data at unnecessary risk.

13. If these allegations are true then they would raise serious concerns about data protection practice. However, so far, none of the allegations or suggestions made has been specific enough to form the basis for investigation by the Information Commissioner. Data controllers have a legal obligation under the DPA to ensure appropriate technical safeguards for the personal data they process. In addition, data controllers are advised to consider that, over time, what once may have been considered strong encryption can become increasingly open to attack

14. When considering access to encrypted communications it is important to bear in mind that any move to make sure that communication service providers or those who send or receive communications use encryption in such a way that the communication can be made available to the UK security services renders the data vulnerable to access by those with malicious intent. In the age of global communications it is simply not possible to ensure that any access to encrypted data is only available to the security services of states with lawful oversight and not to those with less noble motives.

International Data Flows

15. Modern communication mechanisms do not respect national boundaries even if both endpoints of the communication are within the same national jurisdiction. The revelations by Edward Snowden have provoked widespread concerns, not least amongst privacy and data protection commissioners around the globe, about the extent to which the surveillance activities of one country can extend to communications that are neither sent from nor directed to that country.

16. There has been particular concern within the European Union. The ICO has been working with other data protection authorities as part of the Article 29 Working Party on a common response. This has resulted in a Working Party Opinion addressing the

applicability of EU law to surveillance activities generally and in particular to surveillance of electronic communications, including metadata. The Opinion discusses some specific questions including the conflict of laws that can be involved in transfers of personal data from within the EU to public authorities in third countries and the extent to which the national data protection authority has a regulatory role in the area of surveillance.

17. The problem of conflict of laws occurs when the law of a third country requires the transfer of personal data within the scope of EU law to the third country even though such a transfer would be contrary to EU law. A business in the UK faced with a demand to provide data to, for example, facilitate the surveillance activities of a US law enforcement agency may breach US law if it fails to supply the data and breach UK law if it does so. This is currently an issue in relation to the collection of Passenger Name Record (PNR) data both in the EU and elsewhere. It is also the subject of an ongoing legal case in the US being pursued by Microsoft Corp. Such conflicts of law where the surveillance demands of one country conflict with the privacy protections in another can only be resolved through political agreement at international level. In an EU context they cannot be resolved simply by amending EU data protection law or by bringing the data protection authorities into the equation. This is currently an issue in discussions on the proposed new EU data protection legal framework but it would be false to expect that the problem will be resolved once these discussions are concluded. Indeed in may be the case that the problem is exacerbated.

18. Another problem concerns the impact of the surveillance activities of third states on the legitimate transfer of personal data from the UK and other EU countries to those third states. As a general rule 'adequate protection' must be provided for such transferred data in the receiving third state if the transfer is to be a legitimate one under UK law. Broadly 'adequate protection' means protection for the data that is similar to the protection that would have been afforded to the data had they remained in the UK under the protection of UK law. However if the agencies of the third state have unfettered access to the transferred data for surveillance or other purposes it is hard to see how adequate protection can be provided in that state. This is a particular problem in connection with the US Safe Harbor, which is an agreement between the European Commission and the US Government under which an 'adequate' safe haven is provided for data transferred from the EU to businesses in the US. The problem is not though confined to the Safe harbour. It applies similarly to transfers under other mechanisms for ensuring 'adequacy' such as contract clauses and

to transfers to states other than the US. Discussions are still going on between the European Commission and the US Government on the future of the Safe Harbor but if the issue of access by US authorities to the transferred data is not resolved the Safe Harbor agreement could be suspended or terminated. This would have a significant impact on the transfer of personal data between the UK and the US and adversely affect many businesses.

Big Data

19. Another risk to privacy, whether in the context of state surveillance or otherwise, is big data analytics which is developing rapidly. Although some of this may not involve personal data at all, there are many examples of big data analytics that do involve the processing of personal data from sources such as social media, loyalty cards and clinical trials. A key feature of big data is using 'all' the data, which contrasts with the concept of data minimisation in the data protection principles. This raises questions about whether big data is excessive, while the variety of data sources often used in the analysis may also prompt questions over whether the personal information being used is relevant and whether the purpose limitation principle is respected. The Information Commissioner has published a consultation paper on big data albeit not specifically in the context of surveillance activities.[5]

Statutory oversight

20. The current legal and regulatory regime is fragmented and needs review to ensure that it is fit for purpose in providing appropriate and effective oversight and redress mechanisms, proportionate to the surveillance techniques and technologies in use today and those likely to be in use in the foreseeable future. This has also been emphasised by the Intelligence and Security Committee in its report 'Privacy and Security: A Modern and Transparent Legal Framework'.

21. It is important to note that data protection legislation does not provide an absolute right to privacy but does provide a balanced set of safeguards. It also includes exemptions from the full requirements of the DPA in certain circumstances such as where national security interests are engaged (Section 28). The 'national security' exemption applies to any or all of the substantive provisions of the DPA and can be relied on so far as the exemption is required for the purpose of safeguarding national security.

[5] https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf

22. Reliance on the exemption is not dependant on a certificate signed by a Cabinet Minister but such a certificate has to be treated by the Information Commissioner and others as conclusive evidence that exemption is required from the provisions specified in the certificate. An individual can only challenge a certificate by means of an appeal to a specially constituted Tribunal, under judicial review principles. Whilst it is not a specific requirement to put a Certificate in place the Information Commissioner suggest that it is good practice to do so, particularly if the exemption is to be relied on routinely. It is important to note that 'national security' is not defined in the legislation. It can therefore be unclear how far any processing that relies on this exemption is truly for the purpose of protecting the security of the nation as opposed to an arguably lesser purpose such as the prevention or detection crime for which an alternative, narrower exemption is available. The Commissioner has only limited knowledge of the extent to which section 28 certificates are used and they are not reported to him routinely. There is a case here for stronger oversight of their use, including greater transparency.

23. Whilst the national security exemption is a significant limitation on the application of the DPA, other specific regulatory oversight mechanisms do apply including RIPA which provides for oversight by the Interception of Communications Commissioner and the Intelligence Services Commissioner. Furthermore the Justice and Security Act 2013 established greater oversight by both the Intelligence and Security Committee and by the Intelligence Services Commissioner. However this proliferation of oversight mechanisms and regulators with, in some cases, overlapping responsibilities does means it is a complex framework that does not necessarily serve the public well as it is not always clear to individuals who they should raise their concerns with. The Information Commissioner has worked with the other Commissioners to produce a roadmap to assist individuals to navigate the complex landscape of legislative oversight including the Commissioners' roles and responsibilities.[6]

24. Effective oversight and redress is an essential component in inspiring and maintaining public trust and confidence in surveillance activities. Although the application of the Freedom of Information Act to matters of national security is restricted, the principles of openness that underpin this legislation are relevant when considering how far the public bodies involved in security and intelligence activities can and should be transparent and accountable.

[6] https://ico.org.uk/media/for-organisations/documents/1042035/surveillance-road-map.pdf

25. The recent Investigatory Powers Tribunal decision ([2015] UKIPTrib 13 77-H) found that the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which had been obtained by US authorities pursuant to their Prism and/or Upstream programmes had contravened Articles 8 or 10 ECHR although it does now comply. This decision highlights the need for effective regulatory oversight and increased transparency of the activities of the security agencies. In particular the length of time for which an unlawful regime remained in place and the fact that it only came to light as the result of a complaint pursued by a determined complainant strengthens the case for the introduction of a more effective and transparent regulatory system. Any such system must be capable of keeping up with and regulating the increased surveillance capability that developments in communications technology and its use by individuals very often brings.

26. The EU data protection authorities in their Article 29 Working Party Opinion WP215 have called for more effective and independent supervision of intelligence services. This includes key elements such as effective parliamentary scrutiny, and effective, robust and independent external oversight, performed either by a dedicated body with the involvement of the data protection authorities or by the data protection authority itself. This is in addition to strong internal checks within security services for compliance with the national legal framework[7].

27. Ensuring greater independent prior authorisation, subsequent supervision and accountability of surveillance activities becomes more pressing the more intrusive and covert the activity.

Safeguards

28. It is important to note that even where there is a lawful basis for undertaking any surveillance activity, consideration of the wider ethics of the surveillance needs to be a key part of the process. The security services should be increasingly asking themselves not just what can we do and what are we allowed to do but also what should we do. It notable that the National Security Agency in the United States has committed to considering civil liberties and privacy as part of its mission and has appointed a full-time Civil Liberties and Privacy Officer . Her role is to help ensure that security and privacy are not seen as competing objectives and that not only the law but wider privacy and civil liberties considerations

[7] P13. Article 29 Working Party Opinion 04/2014 (WP215) on surveillance of electronic communications for intelligence and national security purposes – 10 April 2014.

are a key factor in strategic decision making. The Civil Liberties and Privacy Officer also has a public facing role contributing to greater transparency and the development of trust and confidence in the NSA's activities.

29. Adopting a 'privacy by design' approach which aims to minimise intrusion and information risks through use of technological and other safeguards is also important. Using technology to help enhance privacy not just to erode it is certainly possible and can help meet the twin objectives of security and privacy protection. The potential for this was recognised in the Government's Draft Communication Bill published in June 2012 which included provisions for the establishment of a 'request filter'. This would have ensured that only information of concern is passed on to investigative bodies without the need for any intrusive or unreliable human intervention and would have allowed communications data of no concern to be promptly deleted. Recent reports have though suggested that security agencies are performing in quite the opposite way through building their own collection, storage, filter and analysis mechanisms.

30. Undertaking a Privacy Impact Assessment is necessary to properly understand the privacy risks involved in any privacy intrusive activity. The process includes consideration of how the privacy risks can be mitigated against through, amongst other things, consulting with those who may be affected by the processing. Whilst the Commissioner has a reasonable level of knowledge about the use of privacy impact assessments by central government departments it is unclear to him whether tools of this type are used by the security services and what other processes they may use in making decisions that impact on privacy.

31. The Information Commissioner has previously drawn Parliament's attention to the need for greater transparency and accountability and has also pointed to the need to adopt a 'privacy by design' approach to use the power of technology to minimise privacy intrusion. The Intelligence and Security Committee has also emphasised and recommended that there should be greater transparency in connection with the work of the Agencies. The need to adopt these measures together with the other safeguards described above is becoming ever more pressing as technological capabilities increase and more and more innovative uses for the technology are explored and put into practice.

Christopher Graham
Information Commissioner
16 March 2015