The Information Commissioner's submission to the Intelligence and Security Committee of Parliament

Privacy and Security Inquiry

Summary

- State surveillance of individuals' communications, whether content or metadata , engages significant privacy and data protection concerns
- The Data Protection Act provides only limited reassurance as a wide ranging exemption from its provisions can in any case be relied on where safeguarding national security is concerned
- 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 communications technologies and networks in use today and likely to be in use in the foreseeable future
- There is a need for greater transparency and accountability
- A 'privacy by design' approach should be adopted to utilise the power of technology to minimise privacy intrusion
- A need to adopt all these measures has been heightened by recent revelations

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 Regulations (PECR) and elements of the Data Retention (EC Directive) Regulations 2009.

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 Committee's Inquiry is focussed on the laws which govern the intelligence agencies' ability to intercept 'private' communications or otherwise process communications data. The term 'private' is not defined in existing legislation and the term suggests that a 'public communication' would be outside the scope of the Inquiry. PECR, the Regulation of Investigatory Powers Act (RIPA) and the draft Communications Data Bill

all refer to 'communications data' and it is assumed the Inquiry extends to such data. It is also noted that the Committee is considering the appropriate balance between an individual's right to privacy and the collective right to security. The Information Commissioner's evidence will therefore focus on the Data Protection Act and how, with certain safeguards in place, the privacy of individuals can be protected whilst giving due weight to the importance of ensuring the security of citizens. Although the application of FOIA to matters of national security is restricted, the principles of openness that underpin this legislation will be relevant when considering how far the public bodies involved in security and intelligence activities can and should be transparent and accountable.

4. Information about an identifiable individual within the content of a communication or within information about a communication is likely to be personal data within the terms of the DPA regardless of the type of communications network used for its transmission. The DPA and PECR set legally enforceable standards and safeguards. The legally enforceable data protection principles include requirements to process an individual's information fairly and lawfully through being clear about how personal data is used or disclosed and complying with other legal duties, not retaining excessive or irrelevant personal data and not holding such data for longer than necessary for the purpose it was collected. These considerations are particularly pertinent when substantial amounts of personal data about persons who are of no current or likely future security concern are collected.

5. PECR also obliges communications providers to safeguard the security of public electronic communications services and places restrictions on the further processing or disclosure of traffic data relating to a communication. These requirements reflect the public policy and human rights emphasis on the private nature of communications and the need to protect these through robust safeguards.

6. The Information Commissioner promotes compliance with these laws, provides guidance, can assess processing for compliance in defined circumstances and handles complaints from individuals. The Information Commissioner also has the power to prosecute and take enforcement action including imposing monetary penalties for serious contraventions of the law.

7. It is important to note that data protection legislation does not provide an absolute right to secrecy or privacy in communications. It provides a balanced set of safeguards and includes exemptions from the full force of its provisions for certain processing activities. This includes processing for the purpose of safeguarding national security (s.28 DPA). The exemption, which applies to any or all of the substantive provisions of the DPA, can be relied on in so far as the exemption is required for the purpose of safeguarding national security. A certificate signed by a Cabinet Minister has to be treated as conclusive evidence of the need for exemption from such provisions of the DPA as are specified in the certificate. Such a certificate could have a substantial limiting effect on the requirement to comply with the safeguards mentioned in paragraph 4 above. It is also important to note that 'national security' is not defined in the legislation and so it is 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 being for a lesser purpose such as the prevention or detection of crime for which a separate, less sweeping exemption is available.

8. There is no requirement to make public the existence of a ministerial certificate and this may only become apparent when the ICO is investigating a specific complaint. This underscores the need for greater transparency and accountability measures. A ministerial certificate can be challenged in the National Security Panel of the Tribunal established to deal with information rights appeals. However, appeals of this nature have been the exception.

9. 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. Effective oversight and redress is an essential component in inspiring and maintaining public trust and confidence. Whilst far reaching limitations on the Information Commissioner's role exist, all the Commissioners and public bodies with responsibility for oversight of different aspects of state surveillance, such as the Surveillance Commissioner and Investigatory Powers Tribunal, meet together on a regular basis. The Information Commissioner has led

work developing and publishing a 'Surveillance Roadmap' to help provide clear guidance for individuals on the regulatory functions of each.[1]

10. The Information Commissioner has also developed working arrangements with government departments to enable him to access the information he needs to see to be able to do his job as a regulator and complaint handler upholding rights of access to information. These arrangements, which minimise the risk of unnecessary disclosure, even to trusted third parties, are embodied in two MOUs signed by the Information Commissioner and the Justice Secretary last year.

11. In addition to specific legislation focussed on personal information and communications, public authorities have to comply with the requirements of the Human Rights Act 1998 (HRA). This gives full effect to the European Convention on Human Rights. Article 8 makes clear that everyone has the right to respect for their private and family life, home and correspondence which includes the content of and information about communications. This is not an absolute right and can be interfered with where this is in accordance with the law and necessary in a democratic society to address a pressing need such as national security. Any such interference must be both necessary and proportionate to meet that need. Observance of these principles should be the cornerstone of any legislative approach to regulating state surveillance. It is important also that a regular review of observance of these principles is built into any oversight mechanism to take into account developments that occur over time such as the changing nature of what is a pressing social need and ever increasing technological capabilities.

12. The Information Commissioner and his predecessors have been concerned about the increasing surveillance of UK citizens in many different contexts. A report on 'the surveillance society' was commissioned in 2006[2] 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

[1] http://ico.org.uk/~/media/documents/library/Corporate/Practical_application/surveillance-road-mapV2.pdf
[2] http://ico.org.uk/about_us/research/reports_to_parliament

and highlighting the Information Commissioner's view on key regulatory and other responses that could usefully be adopted[3]. Both reports were produced by the Surveillance Studies Network, a group of respected academics in this field. Whilst the brief was to consider surveillance in its wider and developing context, both reports covered telecommunications surveillance. Both reports identified flaws in existing safeguards and made many constructive suggestions for improvement.

13. The Information Commissioner 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 of particular relevance to concerns about the propriety and effectiveness of the current legal framework included:

- Increased adoption of 'privacy by design' approaches to minimise intrusion
- A requirement for a privacy impact assessment 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
- 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

3 http://ico.org.uk/about_us/research/~/media/documents/library/Corporate/Research_and_reports/surveillance_report_for_home_select_committee.ashx

14. In addition to concerns about the legal framework, the Committee's call for evidence questions the comparative level of intrusion between different forms of surveillance and how the balance should be struck between an individual's rights to privacy and the collective need for security. Any intrusion into the privacy of citizens, whether this be by way of Closed Circuit Television (CCTV), Automatic Number Plate Recognition (ANPR) cameras or monitoring communications, will engage fundamental human rights concerns and needs to comply with Article 8 of the European Convention of Human Rights. Any processing of personal data, including the collection of data and access to stored data, safeguards and needs to be necessary, proportionate and justified with effective oversight arrangements in place. The extent of these safeguards will depend upon the nature of the surveillance activity concerned. For example public space CCTV surveillance is largely conducted in an overt manner with signs alerting individuals to its presence. 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. Retracing the daily movements of a specific individual from mobile phone records is a far easier option than searching through CCTV data. Furthermore, interception of an individual's communication or communications data can be achieved so covertly that it can be without knowledge of the individual or even the communications provider. Ensuring greater independent prior authorisation, subsequent supervision and accountability is more pressing the more intrusive and covert the activity.

15. It can be misleading to try to compare the varying levels of intrusion caused by different forms of surveillance as the level of intrusion can often be contextual. CCTV in a swimming pool changing area may generally be more intrusive than its use on a busy public street. However to an individual a record of where they are at a particular time, even if in a public place, can engage substantial privacy concerns. It might, for example, show them entering the premises of an organisation of a particular type, such as a health clinic, support group or place of religion. Importantly, in the case of CCTV, surveillance of the individual ceases once they have exited the field of view of the camera(s). It is simply not the case that a CCTV camera is collecting data of every action of every individual.

16. Similarly it is wrong to assume that accessing the actual content of a communication made by phone or over the internet is necessarily more privacy intrusive than acquiring what is known as metadata.

17. 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[4] highlighting the potentially intrusive nature of metadata. It is for this reason that the long standing presumption that less stringent safeguards are required in relation to the collection, recording and analysis of communication data or metadata by the state than are required for access to for the content of communications needs to be called into question.

18. 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 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 suggested that security agencies are performing quite the opposite by building their own collection, storage, filter and analysis mechanisms.

19. 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. Within the European Union where there

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

has been particular concern, the ICO has been working with the national data protection authorities of other EU member states on a common response through an Article 29 Working Party Opinion (to be published shortly). This will address the applicability of EU law to surveillance activities generally and more specific aspects such as transfers of personal data from within the EU to public authorities in third countries where the national data protection authority has a regulatory role that is clearly set out in EU and national law. The problem is where the law of a third country requires the transfer of personal data within the jurisdiction of EU law to the third country even though such a transfer is contrary to EU law. Any such conflict between national law and the law of a third country which prevents the data protection authority's actions from having effect is a serious matter. If, contrary to UK and EU law, the privacy rights of UK and EU citizens are being undermined through the activities of overseas governments, then this needs to be addressed at an international level by the states affected. This conflict of laws cannot be resolved simply through an update of individual national or even EU laws and regulatory powers but requires one or more far reaching international political agreements.

20. One area of particular concern which has been raised as a result of the Snowden revelations is encryption and the exploitation of software vulnerabilities by the security services in order to access or intercept communications and communications data. The use of encryption is highly recommended by the Information Commissioner to provide protection against unauthorised access to personal data. Many breaches of personal data reported to the Information Commissioner could have been prevented if the data controller had adequately addressed vulnerabilities in their information systems or applied effective encryption techniques. Allegations that the security services have required commercial providers deliberately to introduce vulnerabilities or to intentionally choose default parameters or algorithms 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 such 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. 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 to provide appropriate technical safeguards for the personal data they process. The Information Commissioner is updating his advice to data controllers on encryption to indicate which of the various algorithms, key sizes and parameters offer protection that can still be trusted. He is also reminding data controllers that, over time, what once may have been considered strong encryption can become increasingly open to attack.

21. In conclusion, 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. 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 communications technologies and networks in use today and likely to be in use in the foreseeable future. The Commissioner has previously drawn Parliament's attention to the need for greater transparency and accountability and has suggested specific measures to help ensure this is achieved in practice. He has also pointed to the need to adopt a 'privacy by design' approach to utilise the power of technology to minimise privacy intrusion. The need to adopt all these measures has been heightened by recent revelations. At international level we will continue to cooperate with our data protection authority colleagues to develop effective common approaches.

Christopher Graham
Information Commissioner
31 January 2014

Annex A

GLOSSARY

Article 29 WP	The Working Party of EU Data Protection and Privacy Commissioners established under Art. 29 of Directive 95/46/EC
DPA	Data Protection Act 1998
FOIA	Freedom of Information Act 2000
ICO	Information Commissioner's Office
PECR	Privacy and Electronic Communication Regulations
PIA	Privacy Impact Assessment