Intelligence and Security Committee:
Privacy and Security Inquiry

Friday 7th February.

Submission by Open Rights Group

Contact: Jim Killock, Executive Director, jim@openrightsgroup.org

Summary

1. Open Rights Group promotes human rights and civil liberties in the digital age. Founded in 2005, we are now sustained by over 2,000 individual paying supporters, with an Advisory Council featuring leading technology and other industry experts, politicians and writers. In addressing the below issues, we draw on a number of previous pieces of work:

1. ORG's submission to the Joint Committee on the Draft Communications Data Bill[1] (2012)
2. Our report Digital Surveillance: A call for targeted and accountable investigative powers[2] (2013)
3. Our submission to President Obama's Surveillance review group[3] (2013)

2. The disclosures associated with Edward Snowden have revealed that surveillance by our intelligence agencies is not covered by adequate laws, that the existing laws ostensibly designed to cover surveillance are badly outdated, and that there are serious weaknesses in processes designed to provide oversight and accountability.

3. As a result current surveillance practices and laws do not adequately take account of peoples' privacy rights. Mass surveillance is seemingly undertaken in the pursuit of broad aims and objectives such as 'national security' and 'serious crime', governed by laws that have been rendered out of date by changes in technology and weak democratic oversight. This is a toxic and unacceptable combination.

4. We do not accept that there is a 'balance' to be found between 'individual' privacy rights and 'collective' security. Security and privacy rights both bring individual and collective benefits. Privacy rights generate *collective* benefits that are vital for a healthy democratic society. To ensure we reap these benefits, new laws are required to make surveillance more targeted and more accountable and to ensure it is overseen by more powerful, independent bodies.

Response to Committee questions

a.) What balance should be struck between the individual right to privacy and the collective right to security? How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras? To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find

1 https://www.openrightsgroup.org/assets/files/pdfs/consultations/ORGCDBJointComm.pdf
2 https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/
3 https://www.openrightsgroup.org/ourwork/reports/response-to-us-surveillance-review-group

those which might threaten our security? How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?

5. This is a very broad set of questions. We have attempted to break down our response by subquestion.

i. **What balance should be struck between the individual right to privacy and the collective right to security?**

6. The framing of this question is wrong and unhelpful. We disagree that it is possible to distinguish between the *individual* right to privacy and the *collective* right to security. To accept this distinction is to set up a false confrontation between freedoms and obligations. Such a framing is based on a misunderstanding of privacy's value.

7. Rights that seemingly apply to individuals like privacy or freedom of expression also have collective benefits and create social goods. One person having broad protections for their speech enriches public debate. Such protections ensure people can challenge widely held ideas and that those in power cannot easily stifle criticism.

8. Similarly, privacy rights bring collective goods. The right to privacy is a foundation for many things that a tolerant, liberal democracy depends upon.

9. For example, having some control over who is party to one's political conversations one is engaged in helps to support free thinking and debate. Privacy is not just about being cut off from other people, but can be about controlling who has access to personal space. People moderate or adapt what they say depending on their audience. A space in which one is fairly certain of privacy – meaning, certainty about who will hear what you have to say – helps encourage the freer development and exchange of ideas.

10. To give a more concrete example, if journalists feel that their privacy is jeopardised, they will inevitably feel inhibited in the things they can write or say, fearing recriminations for them or their sources. Undermining the privacy of journalists can therefore quickly undermine a free, independent and vibrant press.

11. Further, 'security' for individuals includes the right to encrypt or otherwise protect their data and reduce risks from criminality. Undermining encryption opens vulnerabilities that can be exploited by people with malign intentions, and weakens security for everyone. Thus the attempt to protect collective security in this way damages individual and collective security in other ways. To underscore this point, we quote from an open letter sent by US researchers in cryptography and information security:

> "These are not hypothetical problems; they have occurred many times in the past. Inserting backdoors, sabotaging standards, and tapping commercial data-center links provide bad actors, foreign and domestic, opportunities to exploit the resulting vulnerabilities."[4]

12. The social benefits of privacy rights were recognised by the United States' President's Review Group on Intelligence and Communications Technologies in their final report when setting out the goals to which the United States should aspire:

4 http://masssurveillance.info/openletter.pdf

> "Free debate within the United States is essential to the long-term vitality of American democracy and helps bolster democracy globally. Excessive surveillance and unjustified secrecy can threaten civil liberties, public trust, and the core processes of democratic self-government."

13. So we disagree with this inquiry setting up a confrontation between an 'individual' privacy right – or a right that only benefits the individual to whom it applies - and the 'collective' value of security. In addition to the individual benefits, we urge you to consider the social benefits of strong privacy rights.

ii. How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras?

14. We are unsure about what 'this' refers to in the question. Assuming it refers to the word 'balance', we do not believe there is a 'balance' to be found that can be applied across contexts.

15. An analysis of the nature of the information gathered from internet surveillance, specifically regarding the differences between 'communications data' and 'content', are addressed in answer to part iv of this question below.

16. We would highlight two important changes in forms of surveillance now available. First, more information about people is now available to intelligence agencies than ever before. That information is also far more detailed, and paints a more intimate and detailed picture of somebody, than the information available in the pre Internet age for which current laws were written.

17. Second, it is now easier than ever to link and cross-reference datasets, creating more powerful insights and making more powerful queries of data possible. When thinking of differences between older surveillance techniques or equipment such as the CCTV available to date, these two factors are important to remember.

iii. **To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security?**

18. Suspicion-less, mass surveillance is not proportionate. Surveillance is only legitimate when it is targeted, authorised by a warrant, having been judged by a court to be necessary and proportionate.

19. On this matter we agree with the draft report on the "US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", from the European Parliament's Committee on Civil Liberties, Justice and Home Affairs:

> "...mass surveillance has potentially severe effects on the freedom of the press, thought and speech, as well as a significant potential for abuse of the information gathered against political adversaries;"[5]

5 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-526.085%2b02%2bDOC%2bPDF%2bV0%2f%2fEN

20. The assumption in the question is that mass surveillance has or can help tackle threats to national security, to the extent that these benefits outweigh concerns about the negative societal effects. It should concern Parliament that the benefits and effectiveness of surveillance programmes undertaken by GCHQ are accepted on trust.

21. Parliament should have mechanisms to directly call GCHQ to financial account and to ensure their significant budget is spent effectively, as they seek to do with bodies such as the BBC. This is especially important at a time of austerity-related budgetary pressure. Parliament should consider how to assess the basic effectiveness of GCHQ programs in addition to considering their social impact and justification for them.

22. We would also like to note that the collection of information through surveillance programmes is in itself an infringement of privacy. It is not only the access to and use of that data that needs to be subject to controls and safeguards, and it is not only through 'access' to data that the activity becomes 'surveillance'. For instance, there are inevitable vulnerabilities to large stores of data, with the risk of malign or accidental access, disclosure or loss, and a danger of function creep[6].

iv. **How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?**

23. The Home Office and others argue that content is distinct from communications data, to the extent that less stringent rules for the collection of and access to such data are justified[7]. We disagree, for a number of reasons. 'Communications data' is not in any simple sense less intrusive than content. To suggest otherwise is unhelpful. In the following, we quote from our written submission to the Joint Committee studying the Communications Data Bill[8].

The 'communications data' available now is more revealing than phone records

24. There is a qualitative difference between the data available now, in the digital age, compared to the data available in the pre-Internet days. Data generated now is of a markedly different *type* to phone records and other traditional types of communications data.

25. A record of a phone call tells an investigator who called whom, when, and where. Even this 'traditional' communications data is intrusive. The Article 29 Working Party of European data protection commissioners argued that the Data Retention Directive (Directive 2006/24/EC) involved “an inherently high risk level that requires appropriate technical and organisational security measures. This is due to the circumstance that availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users’ private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression.”

26. However, the new kinds of 'communications data' (that the Communications Data Bill took as its subject for example) can paint a far more intimate picture of our lives. Details of social media

6 This is point also noted by Paul Bernal in his submission to this inquiry: http://paulbernal.wordpress.com/2014/02/06/communications-surveillance-a-miscast-debate/

7 For example, see https://www.gov.uk/government/news/communications-data-bill-published

8 https://www.openrightsgroup.org/assets/files/pdfs/consultations/ORGCDBJointComm.pdf

communications reveals likely political opinions, lifestyle preferences, social circles, habits and patterns of behaviour.

27. Although only the fact that a particular website was accessed, and not the specific page, is recorded, such information can still speak volumes. The fact that someone repeatedly contacted Narcotics Anonymous, or Gaydar, or a political website goes some way to indicate significant aspects of their identity or personality. By combining email, telephone and web access data, and mobile phone location history, one can therefore deduce a detailed picture of an individual's movements, habits and thoughts – certainly a far more detailed picture than phone records or even the content of a phone conversation could offer.

28. Further, the category 'communications data' does not adequately account for the variety of types of data within that definition, and the intrusiveness of such data – which can range from Oyster card user data to Facebook likes, LinkedIn groups, information about Twitter Direct Messages and so on.

29. It is also important to note that it is difficult in practice to separate content from 'communications data'. For a further discussion of the problems of separating content and communications data see "Briefing on the Interception Modernisation Programme", LSE, 2009.

30. So separating out content does not simply reduce the intrusiveness of data to the extent that blanket collection and weaker safeguards than apply to content are acceptable or proportionate.

b) Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted.

31. The Snowden revelations provide further evidence that the laws governing surveillance are out of date. Technology has enabled surveillance practices that the law does not adequately cover. The amount of information now available, and the nature of it, is radically different to when the laws were passed. The laws give surveillance agencies too much scope to collect too much information about too many people with too little in the way of oversight or accountability.

32. Some of these questions have been articulated well in submissions made as part of our joint legal challenge and by the legal advice provided to the All Party Parliamentary Drones Group[9]. For instance, how valid is the distinction between internal and external communications given the international nature of internet infrastructure, and how has this distinction been interpreted in practice? We have yet to see such questions addressed in Parliament.

33. Open Rights Group, alongside English PEN, Big Brother Watch and Constanze Kurz, instructed a legal team to pursue legal action on our behalf and on behalf of all internet users in the UK and EU. This resulted in a case being lodged at the European Court of Human Rights.

34. The basis of our case is that UK surveillance practices are not sufficiently bound by UK law. The Court will decide whether the government's surveillance activities and the existing legislation sufficiently protect the privacy of UK and EU internet users.

9 http://www.tom-watson.co.uk/wp-content/uploads/2014/01/APPG-Final.pdf

35. We argue that the receipt by GCHQ of foreign intelligence data - such as information gathered by the NSA under the PRISM programme – does not seem to be covered by any laws or regulations in the UK. With regard to the TEMPORA programme, we argue amongst other things that the safeguards in RIPA sections 15 and 16 are insufficient and that the generic interception of external communications based simply on the transmission of information by transatlantic fibre-optic cables is inherently disproportionate.

36. On 16th January, the Court wrote to the Government asking them to respond by 2nd May to a number of questions raised by the case. The court also gave the case a rare priority designation. Further information and documents related to this legal challenge, including submissions made so far, supporting expert statements and the response from the court, are available from our website[10].

37. One further factor in whether the laws are 'fit for purpose' is whether they have sufficient democratic legitimacy. So far both the public and Parliament have been left in the dark about the nature of surveillance undertaken in their name, and how existing laws are being interpreted to fit new technological contexts.

38. We have consistently been denied a debate informed sufficiently by legal, technical and budgetary detail. Furthermore, too often the policy makers involved reduce conversations about surveillance reform to questions about whose 'side' participants are on. Both issues were particularly apparent during the debate over the Communications Data Bill[11]. We explained our serious concerns about these issues in our submission to the Joint Committee scrutinising the draft Communications Data Bill[12]. With regard to the work of GCHQ, we note that Lord Blencathra, chair of the Joint Committee, said in response to the revelations about GCHQ activity in October 2013:

> "Some people were very economical with the actuality. I think we would have regarded this as highly, highly relevant. I personally am annoyed we were not given this information"[13]

c) Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

39. Don't Spy On Us is a coalition of groups including Open Rights Group, Big Brother Watch, English PEN, Liberty, Privacy International, Article 19. We believe there are six principles that surveillance should adhere to. Currently surveillance law and practices fall short of these aspirations.

40. First, surveillance is only legitimate when it is targeted, authorised by a warrant, and is necessary and proportionate. Second, whereas currently the Government uses secret agreements and interpretations of archaic laws, we need a clear legal framework governing surveillance to protect our rights.

41. Third, Ministers should not have the power to authorise surveillance. All surveillance should

10 https://www.privacynotprism.org.uk
11 http://www.telegraph.co.uk/news/politics/9719685/Theresa-May-criticised-after-saying-opponents-put-politics-before-peoples-lives.html
12 https://www.openrightsgroup.org/assets/files/pdfs/consultations/ORGCDBJointComm.pdf
13 http://www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance

be sanctioned by an independent judge on a case-by-case basis. Fourth, there should be effective democratic oversight. Parliament has failed to hold the intelligence agencies to account. Parliamentary oversight must be independent of the executive, properly resourced, and able to command public confidence through regular reporting and public sessions.

42. Fifth, innocent people have had their rights violated. Everyone should have the right to challenge surveillance in an open court.

43. Last, weakening the general security and privacy of communications systems erodes protections for everyone, and undermines trust in digital services. Secret operations by government agencies should be targeted, and not attack widely used technologies, protocols and standards.

44. We believe there should be an independent inquiry, concluded prior to election, in order for the government to proceed with legislation that upholds the above principles.

45. The conclusions of two recent US reports are also helpful in looking for further specific changes that could help improve the legitimacy, accountability and proportionality of surveillance in the UK.

46. The US President's Review Group on Intelligence and Communications Technologies[14] argued for increased transparency, with information about surveillance programs made available to the public 'to the greatest extent possible' and legislation that permits telecommunications companies to disclose information about the orders they receive from the government (p18). They recommend 'civilian' involvement in the oversight of surveillance, alongside greater involvement for public interest advocates (p21). And they conclude that the Government should be 'fully supporting and not undermining efforts to create encryption standards...' (p22)

47. We would also point to the aforementioned report from the European Parliament Civil Liberties Committee[15], which again includes a number of helpful recommendations.

14 http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

15 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-526.085%2b02%2bDOC%2bPDF%2bV0%2f%2fEN (see page 19)