Response of the Equality and Human Rights Commission to the Consultation:

Consultation details:

Title:	Privacy and Security Inquiry – Call for Evidence
Source of consultation:	Intelligence and Security Committee of Parliament
Date:	7 February 2014

For more information please contact:

Name of EHRC contact providing response and their office address:	
Clare Collier, Senior Lawyer, Fleetbank House, 2-6 Salisbury Square, London, EC4Y 8JX	
Telephone number:	020 7832 7800
Mobile number:	07968 377824
Email address:	clare.collier@equalityhumanrights.com

Executive Summary

1. The Equality and Human Rights Commission (the Commission) considers that legislative reform is needed on this issue. We consider that an approach to determining when intrusive surveillance should be permitted based on 'balancing' potentially conflicting rights lacks clarity and rigour. Instead it could be helpful to establish a framework of principles which should govern authorisations, including the established principles of necessity and proportionality; and also legitimacy and fairness.

2. While lawful surveillance will sometimes involve interference with the private communications of individuals other than a suspect, the principle of proportionality requires that any collateral interference with others' privacy be as little as is required to assure rights to security and other human rights. We also consider that reforms of the oversight mechanisms could improve the quality and independence of the audit process, which could increase public confidence.

3. Given the already fragmentary nature of RIPA identified in the Commission's 2011 research report,[1] we consider the legal framework governing privacy and surveillance should be the subject of general review rather than piecemeal reform. We have set out at paragraph 28 some specific recommendations both to authorisation of intrusive surveillance and to oversight and accountability processes.

Introduction

4. The Commission welcomes the Committee's inquiry into this important issue. Over recent years the Commission has been involved in relevant research, litigation and briefings. We recently hosted a seminar with invited academic and legal experts to consider the questions posed by the Committee. This response is informed by

[1] Charles Raab and Ben Goold, *Protecting Information Privacy* (Equality and Human Rights Commission Research Report No 69; 2011) at p3.

that range of work, and by our legal analysis of the requirements under the European Convention on Human Rights.

5. Following recent reports concerning mass surveillance programmes by US and UK intelligence services, it is timely to review the legal framework governing access to and interception of private communications in order to ensure that the public interest in privacy and security and individual rights to privacy and security are each properly protected. As we have previously argued, the existing UK law governing the privacy of communications and information privacy more generally is in need of reform. We hope therefore that the Committee's inquiry will provide impetus for such reform.

Questions

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

6. From a human rights perspective, a straightforward juxtaposition of privacy as an individual right and security as a collective one is problematic. The right of each person to be secure from threats to their person is as much an individual right as their right to privacy. The right to life under Article 2 gives rise to a positive obligation on governments to "put in place a legislative and administrative framework designed to provide effective deterrence against threats to the right to life".[2]

7. All human rights are grounded not only in the private interests of individuals but also in the public interest in having those rights protected.[3] Therefore, we place social value on the right to privacy as well as the right to security.[4]

---

[2] *Öneryildiz v Turkey* (2005) 41 EHRR 20 at para 89. Grand Chamber.

[3] See e.g. Joseph Raz, *The Morality of Freedom* (1986).

[4] *House of Lords Constitution Committee, Surveillance: Citizens and the State* (HL 18, February 2009), para 102,: "the widespread use of surveillance may undermine privacy as a public good". See also e.g. JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011) at p20.

8. In this context the Commission also considers that the concept of 'balancing' these rights at the level of general principle should be treated with caution.[5] Rights protect fundamental interests and these interests do not lend themselves to being quantitively weighed in a theoretical way. These two rights are part of a framework of rights, many of which may need to be adjusted to take the others into account. Moreover, the values of privacy and security are to some extent mutually constitutive of one another: a person's enjoyment of privacy depends on that same person enjoying a degree of security against intrusion (from security measures like a lock on a door to legislation against phone hacking). Enjoyment of security can be dependant on having privacy (from personal details being divulged to a violent ex-partner, for example).

9. Respect for the right to privacy plays an important role in maintaining national security. As the former president of the UK Supreme Court, Lord Phillips of Worth-Matravers, said in 2010:[6]

> "The so called 'war against terrorism' is not so much a military as an ideological battle. Respect for human rights is a key weapon in that ideological battle. Since the Second World War we in Britain have welcomed ... millions of immigrants from all corners of the globe, many of them refugees from countries where human rights were not respected. It is essential that they and their children and grandchildren should be confident that their adopted country treats them without discrimination and with due respect for their human rights. If they feel that they are not being fairly treated, their consequent resentment will inevitably result in the growth of those who ... are prepared to

[5] See e.g.*Protecting Information Privacy* n.1 above at p15: "Is it correct to talk about the need for a balance between privacy and the public interest, or does this suggest a false opposition between these two values?"; Jeremy Waldron, "Security and Liberty: The Image of Balance", 11 *Journal of Political Philosophy* (June 2003) 191-210; and David Luban, 'Eight Fallacies About Liberty and Security' in *Human Rights and the War on Terror,* p243: "The supposed 'trade-off' between security and rights is too easy as long as it's a trade-off of your rights for my security."

[6] Lord Phillips of Worth-Matravers, "The Challenges of the Supreme Court", Gresham Lecture, 8 June 2010, pp 37-38.

support terrorists who are bent on destroying our society. The Human Rights Act is not merely their safeguard. It is a vital part of the foundation of our fight against terrorism."

10. Thus, an approach to determining when intrusive surveillance should be permitted by 'balancing' potentially conflicting rights would not be feasible. Instead it could be helpful to establish a framework of principles which should govern such decisions including not only the established principles of necessity and proportionality; but also legitimacy and fairness. Legitimacy and fairness bring into play important considerations relevant to public trust in the system. While it is necessary for details of surveillance operations to remain secret in order to ensure the effectiveness of those operations, more could be done to demonstrate to the public that surveillance decisions are made in a manner that respects fundamental rights. For example, although the Interception of Communications Commissioner is able to review interception warrants made by ministers, he does not review them all and the proportion of warrants he actually reviews in any given year has never been made public.[7]

11. In the individual case, there are long-established principles developed by the courts and applied by public decision-makers for resolving apparent conflicts between different rights. The right to privacy under Article 8 is a qualified right, and therefore open to governmental interference for the sake of legitimate aims such as national security and public safety where necessary. 'Necessity' is qualified both by the values of 'a democratic society', requiring governments to demonstrate a 'pressing social need' for limiting the right,[8] as well as the concept of proportionality, which requires there

[7] See e.g. the 2012 Annual Report of the Interception of Communications Commissioner (HC 571, July 2013) at p 14, where the Commissioner refers to "the total pool of warrants from which I select my samples for review during inspection visits".

[8] See e.g. the judgment of the Grand Chamber in *S and Marper v United Kingdom* (2009) 48 EHRR 50 at para 101: "An interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'".

to be "a reasonable relationship" between "the means and the aim sought to be realised".[9]

12. Security in this context refers not only to the right arising under Article 5 (“Everyone has the right to liberty and security of person. …”) but also the right to life, especially to the State’s positive obligation to preserve the lives of its citizens. The connection is most evident in Article 3 of the Universal Declaration on Human Rights where the concepts are grouped together: “Everyone has the right to life, liberty and security of person”.

13. Although the right to life under Article 2 is framed as an absolute right, an appeal to the use of national security measures to preserve life cannot be treated as a 'trump' over other Convention rights: "not every claimed risk to life can entail for the authorities a Convention requirement to take operational measures to prevent that risk from materialising".[10]

14. It is therefore difficult to set out in abstract terms how these rights should be ‘balanced’. A more specific and contextual approach is needed, but this should be founded on clear principles and be capable of taking account of the variety of contexts. . The current legal framework governing access to private communications extends across a wide range of uses, from the interception of the content of communications by police and the intelligence services under Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA), access to communications data by a broader range of public bodies under RIPA Part 2, and the more general framework governing informational privacy provided by data protection legislation, e.g. the collection of a customer's communications data by a telecom operator or internet service provider. A research paper on information privacy published

[9] See e.g. *Ashingdane v United* Kingdom (1985) 7 EHRR 528 at para 57.

[10] *Osman v United Kingdom* (2000) 29 EHRR 245 at para 166. Just as important, was "the need to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice, including the guarantees contained in Articles 5 and 8 of the Convention".

by the Commission in 2011 warned against attempting to seek a 'one size fits all' approach to questions of privacy.[11]

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

15. It is important to be clear about the scope of the term 'internet communications'. It encompasses very different types of communication, from a text or email message sent from one person to another (analogous to a private letter sent by post), communications between a group of persons who have an expectation of privacy in their shared communications (e.g. a group of friends posting to a private mailing list or forum), communications on social media platforms (whose content may range from highly personal to extremely public, depending on the privacy settings selected), to posting on Twitter or YouTube (which may be tantamount to publishing or broadcasting to the world at large).

16. Each form of internet communication should be considered in its own right, rather than by reference to the particular technology used. For example, a Skype call is more analogous to a telephone call than to an email message (which is, in turn, closer in character to post than to Skype). There are greater similarities between a newspaper article and a news story on the BBC website than between the latter and a private message sent via Facebook, notwithstanding that the second two are both forms of 'internet communications' while the first is not.

17. The Commission would also urge against drawing any straightforward analogy between lawful surveillance of internet communications and that derived from surveillance cameras (also known as CCTV, though often no longer operated within ‘closed circuits’). Although surveillance cameras are increasingly used in a wide range of settings, including shops and restaurants, in the majority of cases they are directed at public places and therefore

[11] *Protecting information privacy,* n.1 above, at p73.

involve different expectations of privacy than would surveillance of private spaces such as a person's home. .Non-recording CCTV in a public place will not infringe Article 8[12]. A similar distinction can be drawn between communications data and content as discussed below.

18. Article 8 categorically provides that every person has a right to respect for his or her private and family life, *including* his or her 'correspondence'.[13] The Court has reiterated that protection for the privacy of a person's correspondence is not limited to letters but extends to phone calls,[14] emails[15] and general personal 'Internet usage'.[16] Whilst changes in communications technology give rise to technical challenges to law enforcement and intelligence services, they do not alter the principles governing the necessity and proportionality of lawful surveillance.

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?

19. Any interference in the right to privacy must be in accordance with the law, necessary in a democratic society and proportionate. Although RIPA does not itself use the term 'reasonable suspicion', the

[12] *Peck v United Kingdom* (2003) 36 EHRR 41 at para 59: "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 ... give rise to an interference with the individual's private life". However, the Court also noted that "the recording of the data and the systematic or permanent nature of the record may give rise to such considerations" (ibid).

[13] See also e.g. Article 12 of the Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"; and Article 17(1) of the International Covenant on Civil and Political Rights: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".

[14] See e.g. *Klass v Germany* (1978) 2 EHRR 214, para 41.

[15] See e.g. *Taylor–Sabori v United Kingdom* (2003) 36 EHRR 17.

[16] See e.g. *Copland v United Kingdom* (App no. 62617/00, 3 April 2007).

European Court of Human Rights has made clear that intrusive powers engaging an individual's right to privacy are unlikely to meet the requirements of Article 8 in the absence of any requirement by the authorities to demonstrate a 'reasonable suspicion' that the individual is engaged in criminal activity.[17] However, lawful surveillance will at times involve interference with the private communications of individuals other than those of a suspect, e.g. those who live and work with the subject of surveillance. Thus it is likely that lawfully targeted surveillance will result in some degree of collateral interference with the communications of persons who are not themselves suspected of involvement in criminal or terrorist activity. Such interference is 'necessary' in the sense that it is unavoidable. At the same time, the principle of proportionality requires that any collateral interference with the privacy of others be as little as is required to assure rights to security and other human rights.[18]

20. Distinguished from surveillance of an individual under suspicion is the so-called 'mass' (i.e. untargeted) collection and monitoring of private communications of the general public on a routine basis for the purpose of data-mining. Undoubtedly this may at times provide useful intelligence about the activities of a small number of suspects within the larger category. However, the legal threshold that a particular measure be "necessary in a democratic society" does not mean merely 'useful', 'reasonable', 'desirable' or 'expedient'.[19] The legislative means adopted to justify a restriction on a fundamental right on the ground of a pressing social need must be no greater than necessary. [20] Unlike the concept of 'reasonable suspicion', which may sometimes extend to a large number of individuals but nonetheless requires some evidential foundation in order to be

[17] *Gillan and Quinton v United Kingdom* (2010) 50 EHRR 45 at para 86: " In particular, in the absence of any obligation on the part of the officer to show a reasonable suspicion, it is likely to be difficult if not impossible to prove that the power was improperly exercised."

[18] See e.g. section 15 of RIPA which requires that disclosure, copying and retention of intercept material be limited to the minimum necessary for the authorised purpose also e.g. the Home Office Code of Practice on the Interception of Communications issued pursuant to section 71 RIPA, para 6.2.

[19] *Sunday Times v United Kingdom (No 2)* (1979-1980) 2 EHRR 245 at para 59.

[20] *R v Shayler* [2002] UKHL 11 per Lord Hope, at para 59

justified, the mass collection of private communications and related data deliberately eschews any form of targeting or selection. It may be possible, for example, for the authorities to have reasonable suspicion in relation to all the residents of a particular building when conducting a surveillance operation but it would be unlikely for the authorities to have reasonable suspicion against all the residents of an entire neighbourhood or city.

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)?

21. There is a long-standing distinction between communications data and the content of communications.[21] In *Malone v United Kingdom* the Court established, firstly, that the collection and use of data from private communications was not as intrusive as the interception and inspection of the content of those communications.[22] Secondly, any collection and use of communications data was nonetheless an interference with the right to privacy and therefore had to be shown to be in accordance with law, necessary and proportionate. In 2010, the Court distinguished between the collection of GPS data and other forms of video and audio surveillance on the basis that the latter "disclose more information on a person's conduct, opinions or feelings".[23]

[21] The terms are used here as they are used in the UK and in the human rights jurisprudence of the European Court of Human Rights.

[22] (1984) 7 EHRR 14 at para 84: "By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8."

[23] *Uzun v Germany* (35623/05, 2 September 2010) at para 52.

22. An unprecedented growth in the volume, detail and quality of 'communications data' has occurred in the past 30 yearsThe definition of 'communications data' under section 21(4) of RIPA now encompasses not just the telephone numbers dialled, and the length of the calls, but also the GPS location data (where the phone call was made or the IP address of the computer that the email was sent from), as well as subscriber data (including the credit card details held by the relevant phone company or ISP).Communications data of a person's internet use (e.g. the names of websites visited and time spent on each site) can disclose highly sensitive information about a person's private life, even if the actual content of the internet usage remains undisclosed.

23. The 'mere' collection of private data about a person is itself an interference with that person's privacy, whether or not subsequently accessed or used.[24] The Grand Chamber held that the blanket retention of DNA samples of innocent individuals once the culprit had been identified was a "disproportionate interference" with their private lives contrary to Article 8.[25] Central to the Court's reasoning was the absence of any suspicion by the authorities against the individuals that was sufficient to justify the retention of their DNA data. In a different case involving the use of stop and search powers by police under section 44 of the Terrorism Act, the Grand Chamber similarly found that the search powers did not comply with Article 8 because of the absence of any requirement on police officers to have 'reasonable suspicion' against the person subject to the search.[26] Although the police or intelligence services may have reasonable suspicions against a number of individuals in respect of the same activity, and this may justify casting a wider net when using surveillance powers, there must nonetheless be some evidential basis to justify the use of surveillance, whether or not that evidence is sufficient to identify a

[24] *S and Marper v United Kingdom* (2009) 48 EHRR 50 at para 121: "the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data".
[25] Ibid, para 125.
[26] *Gillan and Quinton v United Kingdom* (2010) 50 EHRR 45 at para 86.

specific individual, rather than just because it may be useful to the authorities.

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.

24. The Commission considers that some improvements to the legal framework are required. Our report on information privacy assessed RIPA as being "marred by ambiguity, leaving open the possibility of serious errors, inadvertent use of illegal surveillance techniques, and inappropriate use of surveillance powers".[27] Among the problems identified was that access to communications data under RIPA relied heavily on "internal self-authorisation, without the requirement for judicial oversight".[28]

25. Deficiencies in the framework for authorising the interception of communications under Part 1 of RIPA mean that internet communications may be subject to two different interception regimes depending on how they are routed: communications 'internal' to the UK under section 5 RIPA and communications 'external' to the UK under section 8(4). Unlike the 'internal regime' under section 5, there is no requirement for an interception warrant under section 8 to specify that it is targeting a particular individual or premises, meaning that it can encompass broad categories of communications. Section 20 of RIPA defines 'external communications' as a communication 'sent or received outside the British Islands', but this leaves uncertainty about whether internet communications - which routinely involve contact with servers in the US and elsewhere - would be classified as 'external' or 'internal'.

26. When RIPA was debated, the Home Office gave an assurance that communications merely routed through another country would not be

[27] *Protecting information privacy,* n1 above, at (v).
[28] Ibid, p2.

regarded as 'external' communications,[29] and this is supported by the Home Office statutory Code of Practice on the Interception of Communications.[30] However, with the increasingly complex nature of internet communications, it is no longer clear whether such activities as a message posted on Facebook or a search engine request (which involve connection to US-based servers) would constitute an 'internal' communication or an 'external' one.

27. The lower threshold for 'external' communications could impact disproportionately on the privacy of members of those ethnic minorities who are more likely to have relatives overseas and therefore more likely to have their private communications caught by a mass interception warrant issued under section 8(4) RIPA.

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

28. Given the already fragmentary nature of RIPA identified in the Commission's 2011 research report,[31] we consider that the legal framework governing privacy and surveillance should be the subject of general review rather than of piecemeal reform. In the context of interception of communications and access to communications data, we recommend the following measures:

(a) *Authorisation*: serious consideration should be given to introducing a requirement for judicial authorisation for interception warrants under Part 1 of RIPA. Judicial authorisation for such warrants is established practice in the Australia, Canada, South Africa, France, Germany and the

[29] Hansard, HL Debates, Home Office Minister Lord Bassam of Brighton, 19 June 2000: Column 104: "That does not mean that a communication sent and received inside the British Islands may be deemed to be external simply because it takes an international route."

[30] Home Office Code of Practice on the Interception of Communications issued pursuant to section 71 RIPA, para 5.1.

[31] *Protecting information privacy,* n1 above, at p3.

US.[32] Moreover, UK judges already have experience of granting similar applications in relation to asset-freezing in terrorism cases, TPIMs, and (in their capacity as Surveillance Commissioners) in approving authorisations for police to use intrusive surveillance under Part 2 of RIPA. Such a move would ensure effective independent scrutiny of the merits of any governmental request to intercept private communications, and provide evidence that any interference with the privacy rights of affected individuals was necessary and proportionate. In relation to requests to access communications data under Part 2 of RIPA, further consideration should be given to whether requests to access traffic and service use data (but not subscriber data) could meaningfully be subjected to judicial scrutiny.

(b) *Legal certainty*: due to changes in communications technology since 2000, Part 1 of RIPA no longer provides sufficient certainty to members of the public as to when their internet-based communications are liable to be subject to 'internal' interception warrants under section 5 RIPA or 'external' warrants under section 8(4). Parliament should clarify the definition of 'communication' under Part 1 as a matter of urgency.

(c) *Non-discrimination*: the existing scheme of internal and external warrants under Part 1 of RIPA, under which no targeting is required in respect of communications with persons outside the UK, could disproportionately impact on members of some ethnic minorities. It has never been suggested that the requirement for all warrants for the interception of communications internal to the UK to be targeted at either a specific individual or specific premises has prevented the effective use of lawful interception of private communications within the UK. Consideration should therefore be given to introducing a single system of targeted warrants for the interception of communications. The law should

[32] JUSTICE, *Freedom From Suspicion: Surveillance Reform for a Digital Age* (October 2011), p 162.

prohibit the untargeted collection and monitoring of private communications and related data except where there is evidence to support a suspicion and it is necessary and proportionate to do so.

(d) *Oversight*: the current patchwork system of oversight commissioners under RIPA and related statutes, with seven separate Commissioners for the Interception of Communications, Intelligence Services, Surveillance, Information, Biometrics, and Surveillance Cameras. is fragmented, poorly resourced and unsatisfactory. There is a lack of transparency as to the degree of scrutiny provided by the Interception Commissioner, particularly given the number of warrants and authorisations that he is responsible for reviewing annually when measured against the number that he has the resources to review. We recommend the creation of a new, public-facing oversight body, to provide high quality and independent review and audit of surveillance decisions made under RIPA or subsequent legislation and with strong powers to address any unlawful or disproportionate authorisations.

(e) *Accountability*: although we welcome the grant of new powers to the Committee under Part 1 of the Justice and Security Act 2013, further reforms should be considered. As we said during the passage of the Justice and Security Bill[33], appointments to the Committee should be made by both Houses of Parliament and should not be subject to nomination or effective pre-approval by the Prime Minister. The ISC should consult and consider seriously the Prime Minister's and other views as to sensitivity of information, and should be able to redact parts of its reports. However, to ensure the required independence and effectiveness of the role, the contents of reports should be a matter for the ISC, and not subject to effective Prime Ministerial veto or censorship. We are also concerned at the low success

[33] The briefing can be found at http://www.equalityhumanrights.com/legal-and-policy/parliamentary-briefings/justice-security-bill-with-advice/.

rate of complaints before the Investigatory Powers Tribunal, which may suggest problems with the lack of transparency concerning its procedures.

Equality and Human Rights Commission
February 2014