Response to call for written evidence: Intelligence and Security Committee of Parliament

Since 1990 Rights Watch (UK) has provided support and services to anyone whose human rights were violated as a result of conflict. Our interventions have reflected our range of expertise, from the right to a fair trial to the government's positive obligation to protect life. We have a long record of working closely with NGOs and government authorities to share that expertise.

We follow the questions asked by the ISC in its Call for Evidence.

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 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)?

1. The principle of balancing rights lies at the core of both British and European human rights principles. From the Magna Carta to the European Convention on Human Rights, it is clear that some rights are capable of being limited in situations where it is justified. The mechanism for determining these situations is the test of proportionality, whether the imposition of one individual's rights by another is justifiable by being both necessary and proportionate. This means that any interference must be both necessary for the protection of others' rights and be the method of interfering with an individual's rights that has the least impact whilst still achieving the protection of the others rights. In the case of privacy and collective security this means that any invasion of privacy can only be justified if it can be proven to aid collective security and is the least invasive way of doing so.

2. That the interception of communications and other security measures have proven successful in ensuring collective security can be of little doubt, and so that hurdle is not one which we will consider in detail. It can easily be shown that both the data and content of communications will aid in ensuring

collective security. The remaining question is what is proportionate. To answer that, the following questions must be asked; are current investigatory powers the least intrusive method of ensuring collective security; are there other less intrusive methods that could be used; are current investigatory powers nuanced enough to ensure that the level of surveillance can be tailored to the level of threat an individual poses to collective security; and are sufficient safeguards in place to mitigate the infringement on individuals' rights, reducing the impact of any infringement by ensuring that it is well regulated. We will apply this test to the situations found in the ISC's first question.

3. Closed-circuit television (CCTV) cameras allow public bodies and private individuals to monitor specific areas or situations where the cameras are deployed. This allows the user to gain information about individuals who pass through that area, and what activities they undertake whilst in view of the camera. As such, they interfere with an individual's right to privacy. However this intervention is minimal, the camera cannot determine the identity of individuals nor link it to other activities of an individual without additional input. This makes it difficult for a CCTV system to gain private or sensitive information about an individual unless the user holds at least some information about the individual. The intrusion is therefore minimal in most cases, as they merely identify presence in a particular area.

4. It can also be said that most individuals who are filmed by CCTV cameras are aware that they are being filmed, or could easily become aware, and thus have a choice as to how they act when they know they are being watched. Also the use of CCTV cameras is generally confined to public spaces, and is only used where individuals reside in a few highly regulated situations, such as prisons and hospitals. CCTV systems therefore represent a very minimal interference upon an individual's right to privacy in most cases.

5. By contrast internet communications mostly originate from private communications devices. The communications often come from private businesses or private homes. As such the communication contains information that is not in the public domain, unless explicitly put there by the author or recipient of the communication. Many individuals use the internet to communicate private and sensitive information. This information can also, in most cases, be easily attributed to specific individuals or premises. It is very difficult for individuals to tell if their information is being accessed as they cannot see or detect any trace of the surveillance. As such methods of surveillance in relation to internet communications are a great deal more intrusive and should only be justified in limited circumstances.

6. The possibility for gathering sensitive information about private individuals and businesses makes the interception of internet communications similar to

intrusive surveillance, surveillance which is inside an individual's premises or vehicle involving an individual on the premises or using a surveillance device, which does not have to be on the premises if it provides the same sort of data as one on the premises would. It could therefore only be justified in cases where collective security is in clear danger, and if the use of surveillance is well regulated.

7. The monitoring of innocent communications is unlikely to be justifiable. The interception would need to be closely regulated to ensure that it does not overly intrude on individuals' privacy. Individuals must also have a method of challenging the surveillance if they believe that it has been overly intrusive.

8. The difference in intrusion between communication data and content is traditionally that the content of messages contains greater sensitive information about an individual. However this distinction may no longer be valid due to the picture of an individual's life that can be compiled from the large amount of communications data provided by new technology such as smart phones. If the level of sensitivity of information gathered through collation of communication data is similar or equivalent to that gathered through interception of the contents of communication then the distinction all but loses its meaning.

9. We consider that the test of proportionality must govern every decision to use surveillance to gather information on an individual. This is a complex calculation that is hard to legislate, so any regulation must allow discretion to decision makers in the level of surveillance that is appropriate in each case. The use of this discretion must be scrutinised to ensure that high standards of conduct are ensured, and this scrutiny should come from bodies and individuals with a democratic or judicial mandate to make such decisions.

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.

10. In our view the current legal framework governing the security and intelligence agencies' access to the content of private communications is inadequate and must be reviewed and revised.

11. We agree with the Draft Report of the Committee of the European Parliament on Civil Liberties, Justice and Home Affairs 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 dated 8 January 2014 ('the Draft Report').[1]

12. The Draft Report "calls on certain EU Member States, including the UK, Germany, France, Sweden and the Netherlands, to revise where necessary their national legislation and practices governing the activities of intelligence services so as to ensure that they are in line with the standards of the European Convention on Human Rights and comply with their fundamental rights obligations as regards data protection, privacy and presumption of innocence…"

13. The Draft Report continues making particular reference to the UK as follows "… given the extensive media reports referring to mass surveillance in the UK, [the Committee] would emphasise that the current legal framework which is made up of a 'complex interaction' between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000 – should be revised".

14. Our most pressing concern relates to the Regulation of Investigatory Powers Act 2000 (RIPA) which confers a broad catalogue of highly intrusive powers to a wide array of public authorities without any effective oversight, let alone any judicial oversight.

15. Article 8 of the European Convention on Human Rights (ECHR) sets out an individual's right to respect for private and family life and it is the primary ground on which the legality of RIPA may be challenged.

16. In general terms RIPA deals with five different types of surveillance as follows: (1) interception of communications; (2) intrusive surveillance; (3) directed surveillance; (4) covert human intelligence sources; and (5) communications data. Clearly each has a different level of intrusiveness. RIPA sets out the procedures by which various public bodies get these various different surveillance operations authorised. Whilst this second question of the ISC is primarily concerned with the content of private communications we believe serious concerns regarding intrusive and directed surveillance also need to be addressed as a matter of urgency.

17. No RIPA authorisations require application which are subject to judicial scrutiny. For most surveillance techniques the public body exercising the surveillance itself is able to authorise it. This leads to inevitable concerns in relation to independence. The most intrusive form of surveillance, the interception of private communications, requires a warrant issued by the executive. This executive authorisation is a huge concern and is clearly

[1] http://bit.ly/1fWkFwv

inadequate. In order to ensure true accountability judicial scrutiny of applications regarding the interception of private communications is needed.

18. We are particularly concerned by the failure of the regulatory mechanisms within the current legal framework to function adequately. RIPA establishes the Investigatory Powers Tribunal (IPT), the only Tribunal to which complaints about the intelligence services can be directed. The jurisdiction of the IPT includes cases where a public authority (including any of the intelligence agencies) has acted in a way that is incompatible with the Human Rights Act 1998 (HRA).

19. It is our view that the procedures of the IPT are fundamentally flawed. RIPA requires that the IPA carries out all of its proceedings in private.[2] There is no duty to hold oral hearings before which a complainant can be represented[3] and on conclusion the IPA is required only to notify the complainant as to whether they have won or lost.[4] Upon finding in a complainant's favour the IPT is required to provide a summary of its determination including findings of fact. However if a complainant loses the IPT is not required to give any reasons at all. Most shocking however is the fact that there is no right of appeal from the IPT in the UK and rulings cannot be questioned in any court unless the Secretary of State says otherwise.[5]

20. The IPT lacks the necessary independence or power to provide an effective control of RIPA powers. As a result we consider a complete overhaul of the RIPA framework governing the IPA is urgently needed. In technological terms the distance travelled beyond what was envisaged when RIPA was enacted, combined with the failure of the regulatory mechanisms to function adequately, leaves the current framework lacking the sophistication to regulate modern surveillance techniques and forms of communication.

21. Of the five different types of surveillance governed by RIPA, interception of communications has dominated the media since Edward Snowden's revelations regarding the Government Communication Headquarters' (GCHQ's) Operation Tempora (mass surveillance programme) were published in the Guardian in the summer of 2013. The failures of the current legal framework are laid bare in any consideration of GCHQ's Operation Tempora with the existing checks and balances is clearly not sufficient to prevent large scale internet surveillance being secretly carried out on innocent civilians by the government.

---

[2] Rule 9(6) of the Investigatory Powers Tribunal Rules 2000, SI 2665/2000
[3] Rule 9(2) *Ibid*
[4] Section 68(4) RIPA
[5] Section 67(8) RIPA

22. GCHQ's mass surveillance activities are currently under scrutiny both before the IPT and in the European Court of Human Rights[6] and there is wide recognition that the extent of GCHQ's actions was at times unlawful. The mass surveillance techniques used by GCHQ clearly invite scrutiny in relation to the interception of communications however they also highlight issues regarding directed and intrusive surveillance.

23. It has been revealed that information obtained via GCHQ's interception of internet communications has been transferred for use in targeting drone strikes. The advice of Jemima Stratford QC's to Chair of the All Party Parliamentary Group on Drones highlights concerns about the lawfulness of five identified scenarios concerning state surveillance in the UK.

24. Given our work in Northern Ireland, we have particular concern about the civilian use of drones against the backdrop of an inadequate legal framework. It is clear that the developments in surveillance technology necessitate a review of the legal framework governing directed and intrusive surveillance.

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

25. We believe there is a clear case for reform of the legislation governing the collection, monitoring and interception of private communications. To that end we highlight the need for the following:

- The collection of large quantities of data to be regulated separately from the current scheme for the interception of communications data and contents.

- A scheme to regulate the untargeted collection of large amounts of data such as internet communication. This scheme should require that any collection of this sort of data be approved of by Parliament and reviewed by a Parliamentary committee. Any such authorisation should only last for one year, and would require the authorisation of Parliament to renew.

- A scheme to deal with the collection of a large amount of communications data from a single individual. In this case when the communications data collected would allow a reasonable professional investigator to observe or predict an individual's normal day to day life, or to gather sensitive information that could not otherwise be gathered without the use of

[6] http://www.theguardian.com/uk-news/2013/oct/03/gchq-legal-challenge-europe-privacy-surveillance

intrusive surveillance measures, the requirement for regulation should be equivalent to that for intrusive surveillance.

26. When permission for any new surveillance of an individual, group, vehicle or premises is granted the existence of any existing surveillance of that premises should be taken into account when deciding that the new surveillance is proportionate and necessary.

27. The Secretary of State for the Home Department should compile a list of approved intelligence and surveillance techniques, methods and tools, detailing how they intrude upon individuals' privacy. No new technique, method or tool should be added to this list without the approval of 2/3 of the Intelligence and Security Committee. If no consensus can be reached, the measure may be laid before Parliament at the discretion of the Secretary of State.

Respectfully submitted
6 February 2014