AMNESTY INTERNATIONAL

AMNESTY INTERNATIONAL SUBMISSION TO THE INTELLIGENCE AND SECURITY COMMITTEE'S PRIVACY AND SECURITY INQUIRY

INTRODUCTION

"Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society."[1]

1. In June 2013, disclosures made by a former NSA contractor, Edward Snowden, about the nature and extent of surveillance activities by the UK intelligence agency Government Communication Headquarters (GCHQ) and its US counterpart the National Security Agency (NSA), raised serious concerns regarding those states' respect for the right to privacy, and other human rights, notably the rights to freedom of expression and association.[2] The revelations related to three secret surveillance programmes: PRISM (run by the US government's NSA to obtain internet communications from US internet providers); UPSTREAM (direct interception by the NSA as communications passed through the US); and Tempora (direct interception by the GCHQ as communications pass out or into the UK).[3] The revelations included that the UK government receives information from the US that is obtained through PRISM and UPSTREAM.

2. These programmes of mass surveillance are wholly disproportionate and in violation of the UK's human rights obligations. In addition, gaps in UK legislation and oversight mean that there are insufficient safeguards to ensure that communications surveillance is carried out in conformity with international human rights law and standards. Amnesty International therefore calls for urgent reform to the laws governing surveillance, to ensure that intrusions into personal privacy are all properly authorized, comply with human rights principles of necessity and proportionality and are subject to adequate judicial and parliamentary scrutiny.

RIGHT TO PRIVACY AND THE RIGHT TO COLLECTIVE SECURITY

3. The first question posed by the Intelligence and Security Committee (ISC) in its call for evidence is *"what balance should be struck between the individual right to privacy and the collective right to security?"* International human rights law and standards must always guide any response to this question.

4. The right to privacy is reaffirmed in the Universal Declaration of Human Rights (article 12) and guaranteed by the International Covenant on Civil and Political Rights (article 17) and other universal and regional human rights instruments, including the European Convention on Human Rights (ECHR article 8). The UN Special Rapporteur on the promotion and protection of the rights to freedom of opinion and expression has stated that:

> *"Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."*[4]

5. Privacy is essential to a person's liberty and dignity. It is critical to personal identity, integrity, intimacy, autonomy and communication and crucial to personal development and self-fulfilment. Simply put, people are different under surveillance than when they have privacy. Limitations of this right should be strictly justified according to international and European human rights law and standards. Protection of an individual's right to privacy is also a prerequisite for the exercise of other key rights, including freedoms of expression and association. Thus the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has noted that "*The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas.*"[5]Interferences with the right to privacy, such as those caused by interception of individual communications and the mass surveillance of communications, may therefore have a chilling effect on the rights to expression and association.

6. By its very nature surveillance of communications interferes with the right to privacy. It is highly intrusive and strikes at the very heart of a democratic society. Surveillance of private communication, whether of content or metadata, may expose the most private and personal information about individuals, including their family life, sexuality, religious and political beliefs and associations. It may also include communications involving a high expectation of confidentiality, including communications with one's lawyer or doctor.

7. Existing legal frameworks often distinguish between the content of communications and metadata about the communications (ie what website was visited and when or when an email was sent and to whom), suggesting that collection of the latter is not as intrusive or does not infringe the right to privacy in the same way as access to the content of communications would. However, even when the content of individual communications are not monitored, the capacity to analyse data that have been collected in bulk and aggregated from different sources can infringe on an individual's privacy in alarming ways. This is because, when accessed and analysed, communications this kind of metadata can still create a profile of an individual's life, disclosing as much as would be discernible from the content of communications.

8. It has been argued that programmes of mass surveillance are necessary in order to safeguard national security and ensure the protection of its citizens. Amnesty International fully recognizes that the states have obligations to protect the security of its citizens and as a result may legitimately need to resort to covert surveillance, including the interception and monitoring of private communications. However, any surveillance activities must comply with human rights law obligations which balance the needs of the state with the human rights of its citizens

9. In particular, communications surveillance must comply with the general principles of legality, necessity, proportionality and judicial accountability. These principles are not sufficiently respected by programmes of mass surveillance.

LEGALITY: THE CURRENT LEGAL FRAMEWORK REGULATING SURVEILLANCE IN THE UK

10. The ISC has asked "*Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose'…?*"

11. The reluctance of the UK government to provide any detailed information as to how specific aspects of the legal regime are being applied and interpreted in relation to the above programmes of surveillance, beyond referencing generally the Human Rights Act 1998, the Regulation of Investigatory Powers Act (RIPA) 2000 and the Intelligence Services Act, is disappointing.[6] This shows a fundamental lack of transparency by the UK and stymies the possibility of a full and frank debate about communications surveillance and how it should best be regulated in order to comply with states human rights obligations.

12. In general terms RIPA, the primary piece of legislation governing surveillance by public authorities in the UK, does not provide sufficient safeguards to ensure that surveillance is authorized and carried out in conformity with human rights and has proven to be woefully outdated in the face of technological developments.

PRESCRIBED BY LAW:

13. Surveillance interferes with the right to privacy and freedoms of expression and association. For such an interference to interference to be justified it must be "prescribed by law." The law as it stands does not provide sufficient clarity on the legality of surveillance, inadequacies that have only been exacerbated by the rapid developments in technology.

14. When considering whether an interference is "*prescribed by law"* the European Court of Human Rights has set out the following principles: the legal regime governing the interception of communication must be sufficiently accessible, foreseeable, and clear in its terms, so as to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret interference with the right to respect for private life and correspondence.[7] The law must indicate "*with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities*". Rules must be clear and detailed so as to avoid the risk of arbitrary interference and so as to reflect the changing nature of technology.[8] Legal discretion granted to the executive or judge must not be expressed in terms of an unfettered power.[9]

15. There is an absence of adequate legislative controls or safeguards in UK law for the receipt, analysis, use and storage of data received from foreign intelligence agencies that have been obtained by interception. For example, normally, if the UK authorities wished to lawfully intercept emails, telephone calls, and internet data of an individual they would each require a warrant issued by the Secretary of State, which would need to identify the person or premises as the interception subject and which would only last for a limited time. These requirements are laid out in RIPA. None of these safeguards, however, apply if UK authorities solicit or otherwise receive such information from foreign intelligence agencies, as appears to have taken place via the PRISIM and UPSTREAM programmes.

16. There is accordingly no legal regime in the UK that contains sufficiently clear and detailed rules so as to give individuals an adequate indication of the circumstances in which private information obtained by foreign intelligence authorities will be solicited, received, stored, shared, or used by UK authorities. This absence of a published legal structure raises substantial concern that the UK intelligence agencies are able to simply avoid their responsibilities under domestic law simply by cooperating with overseas intelligence agencies.

17. A further concern relates to the Tempora programme and the distinction made in RIPA between "internal" and "external" communications. While the UK government refuses to confirm or deny the existence of Tempora, the programmes appears to be justified by reliance on this distinction that this programme of surveillance concerns external communications, which receive much less protection under RIPA (see paragraph 18 below). No such distinction can be made in practise: the majority of internet-based communications, even within the UK, may be routed through external websites, allowing them to be classified as external communications. Even if the UK government theoretically distinguishes between communications that are truly external and those that remain internal but are routed outside the country it is unlikely that the software would be able to differentiate, meaning that the Tempora programme would effectively collect both internal and external communications. A distinction between internal and external communications therefore cannot be justified for internet-based communication.

18 This dichotomy between internal and external interception appears to allow the UK government excessive unfettered discretion to monitor, intercept and store information shared over the internet. For example, although RIPA 2000 sets out certain protections and requirements for the issuing of an interception warrant, the safeguards that apply to the interception of internal communications are not applicable to external communications.[10] As a result when the UK authorities want to intercept "external" communications, there is no need to identify any particular person who is to be subject of the interception, the particular address that will be targeted, or any other factors for identifying the communications that may be or are to be intercepted. This allows the government to certify surveillance on a massive and unprecedented scale, as appears to have occurred through the Tempora programme, which has reportedly been established under warrants relating to external communications, allowing access to all external communications passing along more than 200 transatlantic fibre-optic cables without restriction.

PROPORTIONALITY:

19. The requirement of proportionality means that interventions must be appropriate to achieve the legitimate aim (such as preventing terrorism or other serious crimes), the least intrusive method of achieving the legitimate aim and must be proportionate to the interest protected. Amnesty International believes that programmes of mass and blanket surveillance, such as those described above, are wholly disproportionate. This is because the interception programmes we are commenting on relate to the mass interference with the private lives of millions of people; potentially all persons with phones and who access the internet in the UK or whose communications pass through the UK. The effect is that the private data of millions of individuals will be monitored, intercepted and analyzed even though the vast majority will have no link to terrorism or other serious crime. This is effectively the most intrusive method of achieving the legitimate aim of preventing terrorism, or other serious crimes and there has been no attempt to utilize less intrusive means, such as targeted interception based on reasonable suspicion.

20. The extent of the interference can be demonstrated, for example, by the fact that under the Tempora programme information is subject to an automatic search against over 40,000 search terms. This means that there is an absence of sufficiently precise criteria for determining when intercepted external communications will be further analyzed and that the interference is not strictly limited to what is necessary and proportionate. In other words it is not possible for such interception to be used only for targeted and sufficiently important purposes as required by human rights law.

21. In addition, the term "national security" has been given a very wide and flexible meaning in the UK and its frequent invocation to justify invasive limitations on the enjoyment of human rights continues to be of serious concern to Amnesty International.[11]

JUDICIAL AND OTHER OVERSIGHT

22. Effective judicial and parliamentary oversight is a key safeguard in ensuring that surveillance is carried out in a human rights compliant manner. As such, it is imperative that when examining the adequacy of the existing legal framework the issue of oversight is also included. Indeed the European Court of Human Right has confirmed that the availability of adequate and effective guarantees against abuse is critical for the determination that the interference is justifiable in a democratic society.

23. There is an ongoing absence of adequate judicial oversight and scrutiny of surveillance activities in the UK, as the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression recently noted.[12] For instance, a long-standing concern with RIPA 2000 is that warrants authorizing the interception of communications are granted by the executive and not by a judicial authority. The lack of independent judicial scrutiny of application for such intrusive surveillance means there is no proper mechanism for accountability and does not comply with human rights principles.

24. Amnesty International believes that limitations in the system of the two Commissioners appointed to oversee the intelligence services mean that they are not adequate to prevent abuse of surveillance powers in UK. For example, the Interception of Communications Commissioner is a supervisory role, which does not have powers to prohibit or quash an interception warrant. The Commissioner examines, ex post, warrants on a random basis and there is no evidence that he has ever examined the TEMPORA programme, nor has he set out any conditions on the use and examination of material obtained from bulk collection of all external communications. As a result though the Commissioner can fulfil a useful watchdog role, it cannot compensate for a lack of judicial or independent authorisation of warrants, particularly in the context of external communications that are subject to minimal statutory conditions and limitations.

25. The Investigatory Powers Tribunal (IPT) also cannot constitute a substitute for independent approval of communications warrants. The jurisdiction of the tribunal is limited to determining complaints referred to them by members of the public and since the granting of external communications warrants are not disclosed individuals are not in a position to challenge them. The IPT is also a highly secretive tribunal that determines its own rules of procedure. For example, when it dismisses a complaint – as it has done in the vast majority of its cases – it does not let the person know whether an interception took place, and the tribunal's decisions cannot be challenged in court. It is crucial that complaints against the intelligence services are heard in as transparent

a manner as possible in order to ensure the accountability of government agencies with respect to surveillance.

26. Finally, with respect to parliamentary oversight it is not clear that the ISC in its current form can play this role effectively. While there have been some improvements to the ISC following the coming into force of the Justice and Security Act 2013, the government still retains the right to withhold information from the ISC and the Prime Minister remains ultimately responsible for deciding what material the ISC can put in the public domain.[13]

---

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, UN Doc: A/HRC/23/40, § 81.

[2] In December 2013, Amnesty International submitted a legal complaint to the Investigatory Powers Tribunal challenging the mass interception of/ interference with communications by the UK intelligence and security agencies. The complaint argues that the activities of the UK agencies are in breach of the UK government's fundamental human rights obligations, principally the rights to private and family life and freedom of expression. A copy of the compliant can be provided to the Intelligence and Security Committee upon request.

[3] For further detail see, amongst others, "NSA Prism program taps in to user data of Apple, Google and others", Glenn Greenwald and Ewen MacAskill, The Guardian, 7 June 2013; "GCHQ taps fibre-optic cables for secret access to world's communications", The Guardian, 21st June 2013; "UK gathering intelligence via covert NSA operation", Nick Hopkins, The Guardian, 7 June 2013. See also the Joint Application by Big Brother Watch and others to the European Court of Human Rights, accessible at: https://www.privacynotprism.org.uk/assets/files/privacynotprism/496577_app_No_58170-13_BBW_ORG_EP_CK_v_UK_Grounds.pdf.

[4] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, UN Doc: A/HRC/23/40, § 22.

[5] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, UN Doc: A/HRC/23/40, § 24.

[6] Secretary of State for Foreign and Commonwealth Affairs (the Rt. Hon. William Hague MP) statement to Parliament on 10 June 2013. (Hansard HC, 10 June 2013, Col. 32-42).

[7] *Malone v the United Kingdom,* (Application no. 8691/79), 2 February 1984, para. 67; *Weber and Saravia v Germany,* (Application no. 54934/00), 29 June 2006, para. 93; *Liberty and others v United Kingdom,* (Application no. 58243/00), 1 July 2008, para. 59.

[8] *Malone v the United Kingdom,* (Application no. 8691/79), 2 February 1984, para. 79; *Weber and Saravia v Germany,* (Application no. 54934/00), 29 June 2006, paras. 93 and 94; *Liberty and others v United Kingdom,* (Application no. 58243/00), 1 July 2008, para. 62; *Kennedy v the United Kingdom* (Application no. 26839/05), 18 May 2010, para. 151; *Iordachi v Moldova* (Application no. 25198/02) 10 February 2009, para 39.

[9] *Weber and Saravia v Germany,* (Application no. 54934/00), 29 June 2006, para 94; *Telegraaf Media Nederland Landelijke Media BV v The Netherlands* (App. No. 39315/06), 22 Novemeber 2012, para. 90.

[10] See section 20 of RIPA 2000 which makes it clear that where the communication is "external", that is either sent or received outside the British Islands, the protections under section 8(1) and 8(2) do not apply.

[11] See, for example, *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153.

[12] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, UN Doc: A/HRC/23/40, § 54

[13] For further discussion of these issues, see, for example, Amnesty International UK response to the Justice and Security Green Paper, January 2013.