Privacy International's submission in advance of the consideration of the periodic report of the United Kingdom, Human Rights Committee, 114th Session, 29 June – 24 July 2015

1 June 2015

1. Introduction

Privacy International notes the UK written replies to the list of issues in relation to the UK's laws, policies and practices related to interception of personal communications.

The following comments are based on Privacy International's expertise on and analysis of the UK's legislation, policies and practices on surveillance and draws from the organisation's litigation in UK courts and the European Court on Human Rights on related issues.

Contrary to the UK government's assertion, the Regulation of Investigatory Powers Act 2000 (RIPA) and other legislation does not ensure that interception and access to communications data is carried out in accordance with applicable international human rights standards to respect and protect the right to privacy, notably Article 17 of the International Covenant on Civil and Political Rights (ICCPR.)

In fact, on 12 March 2015, the Intelligence and Security Committee of Parliament, which has responsibility for oversight of the UK intelligence services, published a report entitled *Privacy and Security: A modern and transparent legal framework* ("ISC Report"). The ISC expressed significant concerns about several aspects of the UK statutory regime regulating the interception of personal communications, including the definition of 'external' and 'internal' communications; the lack of clarity within the existing laws; and the lack of a clear legal framework in relation to the compiling, retention and oversight of databases of communications and related data. It recommended fundamental changes to the existing legislative and oversight regimes in order to address those concerns.[1] While the ISC report did not fully disclose the practices of the intelligence agencies and sought to mask the reality of the UK's mass surveillance practices by describing them as "bulk interception", it still represents an important recognition that reform of the UK surveillance laws is long overdue and

1 The report is available here: http://isc.independent.gov.uk

should be done with the view to limit the surveillance powers to bring them into line with international human rights standards, including notably Article 17 of the ICCPR.[2]

The UK government announced on 27 May 2015 that a new piece of legislation, the Investigatory Powers Bill, will be brought forward in order to update and consolidate existing surveillance laws. Privacy International encourages the Human Rights Committee to make detailed recommendations to the UK to inform the content of this new legislation.

2. Unregulated interception and access to personal communications data

Before addressing the UK's responses to the list of issues, Privacy International would like to bring to the Committee's attention the existence of certain UK surveillance practices which are conducted in the absence of a legal regime that contains sufficient safeguards against arbitrary use. While the secrecy surrounding surveillance activities (combined with ineffective oversight and over-reliance on the "neither confirm nor deny" policy) makes it impossible to provide a full picture, the following practices (acquisition and use of Bulk Personal Datasets and reliance on hacking as a form of surveillance) raise particular concerns for their implication to the right to privacy.

2.1 Bulk Personal Datasets

The March 2015 ISC report revealed for the first time that intelligence agencies acquire and rely on Bulk Personal Datasets, which are massive databases, likely to contain personal information about millions of people, including British citizens. Details of these datasets are scarce, but according to the limited information published in the ISC report "datasets vary in size from hundreds to millions of records" and "may include significant quantities of personal information about British citizens."[3] Acquisition and use is all authorized internally within the UK's signals intelligence agency, the Government Communications Headquarters (GCHQ). Further, until 13 March 2015, there was no oversight body with a statutory role to oversee their use.[4]

2.2 Hacking

Hacking, also known as computer network exploitation (CNE), is an extremely intrusive form of surveillance. It can yield information sufficient to build a total profile of a person, from their daily movements to their most intimate thoughts. It is potentially far more probing than techniques traditionally classified under the Regulation of

2 See Privacy International's statement on the release of the ISC report, available here: https://www.privacyinternational.org/?q=node/505

3 ISC report, page 57.

4 On 13 March, the Prime Minister issued a 'direction' under RIPA to mandate the Intelligence Services Commissioner to monitor these datasets. See Intelligence Services Commissioner (Additional Review Functions)(Bulk Personal Datasets) Direction 2015. Datasets are defined in this directive as follow: a bulk personal dataset means any collection of information which: a) compromises personal data as defined by section 1(1) of the Data Protection Act 1998; b) related to a wide range of individuals, the majority of whom are unlikely to be of any intelligence interest; c) is held, or acquired for the purposes of holding, on one or more analytics systems within the Security and Intelligence Agencies.

Investigatory Powers Act (RIPA) as "intrusive surveillance". It is also rapidly becoming the intelligence services' tool of choice.

The British Government has admitted its intelligence services claim the broad power to hack into personal phones, computers, and communications networks anywhere in the world, even if the target is not a threat to national security or suspected of any crime.[5] The only legal basis for such practice is an extremely broad mandate given to the Secretary of State under the Intelligence Services Act 1994 to issue a warrant to permit any action that the minister believes is necessary "for the purpose of assisting the GCHQ" in carrying out its functions.

In February 2015, the government released a draft Equipment Interference Code of Practice.[6] The draft code offers limited guarantees against abuse.[7] Further, state-sponsored CNE should be fully debated and, if approved, enshrined in primary legislation. Instead, the UK amended the Computer Misuse Act on 3 March 2015, to exempt law enforcement and intelligence services from provisions that make hacking illegal in the UK. The change grants UK law enforcement increased leeway to potentially conduct cyber attacks within the UK without being subject to criminal prosecution. It appears no regulators, commissioners responsible for overseeing the intelligence agencies, the Information Commissioner's Office, industry, NGOs or the public were notified or consulted about the proposed legislative changes. There was no published Privacy Impact Assessment.[8]

3. Privacy International's critique of the UK's reply to the list of issues

Of particular concern to Privacy International, the UK legal regime of interception of communications allows for mass surveillance, discriminates against non-UK residents, allows blanket retention of communications data, and lacks effective redress and robust oversight.

3.1 Mass surveillance

Section 8(4) of RIPA provides for "untargeted" warrants for the interception of "external communications." Such warrants have been used as the basis for the mass interception of millions of private communications as well communications data.

"External communications" are defined in Section 20 of RIPA as communications "sent or received outside the British Islands". The UK government has admitted that it interprets this provision to include any communications via social media so long as the

5 The response is available here: https://www.privacyinternational.org/sites/default/files/Privacy%20Greennet%20Open%20Response%206%20Feb%202015.pdf
6 Available here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf
7 See submission by Privacy International and Open Rights Group, available here: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf
8 See Privacy International, After legal claim filed against GCHQ hacking, UK government rewrite law to permit GCHQ hacking, 15 May 2015, available at: https://www.privacyinternational.org/?q=node/584

server that processes the communication is outside the UK, meaning Facebook and Google users could have their communications captured.[9]

The legal regime for the interception of "external communications" falls short of the three overarching principles of legality, necessity and proportionality. No particular person or target need be specified for the interception to take place, resulting in mass interception of communications. And no additional authorisation is needed before intercepted "external communications" are looked at, listened to or read. There is no prior judicial authorisation and very limited ex post facto oversight.

The ISC report confirmed that, pursuant to section 8(4), the British government intercepts undersea cables (or "bearers" as the report suggests) through which billions of communications flow. No more than 19 general warrants, issued by ministers, cover the entire "bulk interception" regime.

RIPA's "external communications" regime is also discriminatory on grounds of nationality and national origin because of the distinction between internal and external communications, and the special protections granted to people in the UK under section 16 RIPA. As a British person is more likely to be present in the British Islands, a section 8(4) warrant is therefore likely to have a disparate adverse impact on non-British nationals. Moreover, section 16 provides that the only restrictions on intelligence agencies searching through and analysing intercepted data is that they cannot do so on the basis of terms "referable to a person known to be in the British Isles", again creating a protection for persons in Britain and allowing for unrestricted interference with communications of all those persons outside of Britain.

The UN High Commissioner for Human Rights and the UN Special Rapporteur on counter-terrorism and human rights have noted how several legal regimes on interception of personal communications, like the UK, distinguish between obligations owed to nationals and non-nationals and residents and non-residents, providing external communications with lower or non-existent protection, in ways that are discriminatory and incompatible with Article 26 of the ICCPR.[10] The UN Special Rapporteur on counter-terrorism concluded that states "are legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction".[11]

Further, the distinction between internal and external communications is arbitrary and rendered meaningless in the context of the technical architecture of modern digital

---

9 Statement of Charles Farr, the Director General of the Office for Security and Counter-Terrorism, dated 16 May 2014, para 137, available at https://staging.privacyinternational.org/sites/default/files/Witness%20st%20of%20Charles%20Blandford%20Farr_0.pdf

10 See report of the UN High Commissioner on Human Rights on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014; and report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014.

11 Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, paragraph 43.

communications, with messages such as e-mails routed through different countries even if both the sender and the intended recipient are resident in the UK. Tapping fibre optic cables, as the UK is doing, means that vast amounts of both "internal" and "external" communications will be gathered as a by-product of mass interception under Section 8(4) of RIPA. Once collected, there is no statutory requirement on the UK Government to discard, filter or ignore those internal communications.

These concerns are compounded by the fact that RIPA and other relevant legislation regulating the activities of the intelligence agencies (such as the Security Services Act 1989 and the Intelligence Services Act 1994) contain no meaningful safeguards to prevent GCHQ from obtaining the private communications of millions of UK residents from overseas intelligence partners. This statutory lacuna is particularly concerning in light of the close cooperation and sharing of personal communications data between GCHQ and the US National Security Agency (NSA). That access includes both the raw data itself (for example being able to directly search and extract bulk intercepted communications which may never be analysed by the NSA) and access to refined data that has been analysed and collated by the NSA.[12] The unregulated intelligence sharing between the UK and the US, and other countries, bypasses the already weak safeguards that regulate collection of personal data of UK residents under RIPA.

In December 2014, the Investigatory Power Tribunal found that mass surveillance of internet traffic carried out by the UK was in principle lawful. The decision relied on the fact that, during the course of the case, small selective portions of previously secret policies governing the UK's surveillance activities were made public. In a separate, related ruling in February 2015, the Tribunal held that the intelligence sharing between the US and the UK was unlawful prior to the December ruling, because the rules governing the intelligence sharing were kept secret. Privacy International and other human rights organisations appealed the December IPT ruling to the European Court of Human Rights.[13]

3.2 Metadata/Communications Data

Under UK law, there are no meaningful restrictions on the collection of communications data ("metadata"), irrespective of whether they pertain to "internal" or "external" communications, or to residents in the UK or not. Under section 8(4) RIPA, GCHQ

12 PRISM and UPSTREAM have been reported among the programs of mass surveillance employed by the NSA. PRISM enables the NSA to obtain information from some of the world's largest internet companies, such as Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. Information obtained is likely to include the emails, web-searches, phone calls, photos, videos made or sent by individuals in the UK who use any of the products of those companies, or who communicate with individuals using, for example, a Gmail account or other products of internet companies based in the US. UPSTREAM collection involves the direct interception of communications during transmission. It is described, according to NSA presentation slides published in The Guardian, as being the "collection of communications on fiber cables and infrastructure as data flows past".

13 The NGOs application to the European Court on Human Rights is available here: https://www.privacyinternational.org/sites/default/files/HR%20Orgs%20v%20UK.pdf

intercepts and stores communications data and can search through it without any restriction, as the section 16 safeguards described above do not apply to communications data. Furthermore, under Part 2 of RIPA, access to communications data only requires authorisation by a senior official of the public body undertaking the collection. Over 200 agencies, police forces and prison authorities are authorized to acquire communications data under RIPA, and they do so, on average, 500,000 times a year. As a result, it is difficult for individuals to foresee when and by which State agency they might be subjected to surveillance.[14]

The current law regulating retention of communications data, the Data Retention and Investigatory Powers Act (DRIPA), was adopted by the UK Parliament in July 2014, following the judgment of the Grand Chamber of the Court of Justice of the European Union(CJEU) that invalidated the EU Data Retention Directive requiring the bulk retention of metadata as incompatible with the right to privacy.[15]

Failing to take into account the conclusions of the CJEU, DRIPA merely reinstates the previous requirement, established under the Data Retention Directive, of the mandatory blanket retention of communications data of the entire UK population for twelve months by providers of telecommunications services. In addition, the Act contains new powers, including allowing the government to require overseas companies to build interception capabilities into their products and infrastructure. The legislation was passed as an emergency measure, without sufficient parliamentary or public debate. It is currently under judicial review.

As noted in the UK replies to the list of issues, the Counter-Terrorism and Security Act 2015 amended DRIPA, including by giving the Home Secretary the power to require communications companies to retain "relevant internet data".[16] Beyond the blanket

---

14 According to the 2014 Annual Report of the Interception of Communications Commissioner "172 public authorities acquired data in 2014. 88.9% of the applications for communications data were made by police forces and law enforcement agencies, 9.8% by the intelligence agencies and 1.3% by local authorities and other public authorities (regulatory bodies with statutory functions to investigate criminal offences and smaller bodies with niche functions)." Available at: http://www.iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf According to a June 2015 Big Brother Watch's report, more than 700.000 requests for communications data were made by UK police forces between 2012 and 2014. 96% of those requests were granted. The report, based on freedom of information requests, is available here: http://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/05/Big-Brother-Watch-Report-Police-Communications-Data1.pdf

15 Judgment in Digital Rights Ireland case (joined cases C-293/12 and C-594/12) available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

16 Relevant internet data "means communications data which (a) relates to an internet access service or an internet communications service, (b) may be used to identify, or assist in identifying, which internet protocol address, or other identifier, belongs to the sender or recipient of a communication (whether or not a person), and (c) is not data which— (I) may be used to identify an internet communications service to which a communication is transmitted through an internet access service for the purpose of obtaining access to, or running, a computer file or computer program, and (ii) is generated or processed by a public telecommunications operator in the process of supplying the internet access service to the sender of the communication (whether or not a person);". See: http://www.legislation.gov.uk/ukpga/2015/6/part/3/enacted

mandatory data retention regime under DRIPA, this provision requires to retain types of metadata that companies would not routinely hold for billing purposes.[17]

The interception, collection and use of metadata interfere with the right to privacy, as it has been recognized by human rights experts, including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.[18] The CJEU noted that metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[19]

The blanket retention of metadata provided for in DRIPA is in breach of existing EU provisions protecting the right to privacy, such as the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC.[20] Because of its untargeted and indiscriminate scope, DRIPA also fails to comply with the test of necessity and proportionality.

3.3 Lack of prior judicial authorisation

Under RIPA, interception of communications is authorised by a minister, and access to communications data, directed surveillance and the use of covert human intelligence sources by a senior member of the relevant agency. There is only qualified provision for judicial authorisation under RIPA for intrusive surveillance by police (but, notably, not the intelligence services), for requests for encryption keys, and when local authorities seek access to communications data.

Judges are best suited to apply the legal tests that ensure that any interference with the right to privacy carried out by intelligence or security agencies complies with the principles of necessity and proportionality. There is growing recognition by international experts and by national laws that surveillance should only be carried out on the basis of a judicial order.[21] The same independent judicial authority should also ensure that any

---

17 For an analysis of this provision, see Liberty's Second Reading briefing on the Counter-Terrorism and Security Bill in the House of Lords, available at: https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20Briefing%20on%20the%20Counter-Terrorism%20%20Security%20Bill%20%28Second%20reading%20HOL%29%20%28Jan%202015%29.pdf

18 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

19 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

20 See Open Rights Group and Privacy International's submission in the judicial review proceedings against the Data Retention and Investigatory Powers Act (DRIPA), available here: https://www.openrightsgroup.org/ourwork/reports/submission-filed-by-org-and-privacy-international-in-dripa-case

21 UN High Commissioner for Human Rights' report on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014. See also Human Rights Committee, Concluding Observations on the 4th U.S. report, 27 March 2014, para. 22, and European Court of Human Rights, *Kopp v. Switzerland* [1999]

surveillance carried out is in compliance with such order and, more broadly, respects the right to privacy.

3.4 Ineffective oversight and limited access to effective judicial remedy

RIPA provides for the appointment of two Commissioners to supervise the activities of the intelligence services. The Interception of Communications Commissioner is responsible for overseeing the interception of communications and the acquisition of communications data by public authorities (including the intelligence agencies). The Intelligence Services Commissioner is responsible for overseeing the use of other intrusive powers by the UK intelligence agencies.

These commissioners are part-time and lack the resources necessary to effectively monitor the practices of the UK government bodies involved in interception, collection and analysis of personal communications. They are not independent from the government, being appointed by and reporting to the Prime Minister. Further, their public reports do not provide adequate information, such as detailed statistics on warrants and authorisations issued to the security and intelligence agencies. Concerns about their limited powers and capacity have been raised by the ISC and the Home Affairs Committee.[22]

Beyond the commissioners, some forms of oversight of the intelligence services is entrusted to the Intelligence and Security Committee (ISC.) The powers of the ISC are limited (they cannot compel state agencies and government departments to provide information), and its standing is not that of a fully fledged parliamentary committee. Further, the ISC remains under significant executive influence: the Prime Minister nominates its members, approves any investigation by the ISC, reviews the committee's reports prior to their submission to Parliament and may decide that matters should be excluded in the interests of national security. As a result, the ISC has consistently failed in its duty to challenge the intelligence agencies, and, as the Parliamentary Joint Committee on Human Rights (JCHR) has noted, the level of redaction of ISC reports is sometimes so great that "it can be difficult to follow the Committee's work and to understand its reports."[23]

All legal challenges to the use of surveillance powers granted under RIPA are currently heard by the Investigatory Powers Tribunal (IPT) (under Part IV of RIPA). The IPT operates in a shroud of secrecy. The rules regulating the IPT (the Investigatory Powers Tribunal Rules S.I. 2000/2665) provide that "the Tribunal shall carry out their functions in such a way as to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or

27 EHRR 91, para. 74.

22 See ISC report, 2015 and Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 167, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102. htm

23 See *Allegations of UK Complicity in Torture*, 23rd Report of the JCHR session 2008-2009, paragraph 58.

detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services." There is no presumption that hearings will be held in open court unless there is a compelling case otherwise. As a result, the IPT cannot disclose to a complainant the fact that a closed hearing is taking place, the identity of any witness or any information provided at the hearing, unless those attending the hearing, the witness, or the provider of the information consent. The IPT often relies on secret information provided by the intelligence services to reach its conclusions, and fails to disclose this information in a meaningful way to the claimants. Further, if the IPT finds against a claimant it cannot give reasons for its decision. If the tribunal upholds a complaint it is only required to provide the claimant with a summary of its determination.

Before the IPT's judgment in the claim brought by Liberty, Privacy International and Amnesty International in February 2015, it had upheld only ten out of over 1,500 complaints presented by members of the public.

There is no appeal from a decision of the IPT. The Supreme Court of the United Kingdom held that the IPT has exclusive and final jurisdiction.[24]

Recommendations

Based on these observations, Privacy International suggests that the following recommendations for the UK government:

- Take all necessary measures to ensure that its surveillance activities, both within and outside the United Kingdom, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance, which includes refraining from engaging in mass surveillance and adequately and transparently regulating information sharing with intelligence partners;
- Review and reform existing laws regulating surveillance and collection of personal data in order to ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance, and procedures for the use and storage of data collected; and (iv) provide for effective safeguards against abuse;

24 See R(A) v B [2009] UKSC 12; [2010] 2 AC 1.

- Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization and monitoring of surveillance measures, and establish strong and independent oversight mandates with a view to preventing abuses;
- Repeal DRIPA and refrain from imposing mandatory retention of data by third parties;
- Ensure that affected persons have access to effective remedies in cases of abuse.