LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's response to the Home Office consultation on the Interception of Communications Code of Practice

March 2015

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

Bella Sankey
Director of Policy
Direct Line 020 7378 5254
Email: bellas@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sara Ogilvie
Policy Officer
Direct Line 020 7378 3654
Email: sarao@liberty-human-rights.org.uk

Introduction

1. The Interception of Communications Code of Practice (the 'Existing Code') was first published in 2002 and revised in 2010. It provides guidance on the powers and duties contained in Chapter 1 of Part 1 of RIPA which covers the interception of communications. The present consultation concerns an updated Code of Practice (the 'Draft Code') and is premised on the adequacy and lawfulness of the existing legislative framework governing surveillance in the UK: a premise which Liberty rejects.

2. Liberty believes that several aspects of the interception regime under Part 1 RIPA are unlawful and do not comply with the Human Rights Act 1998 which incorporates the European Convention on Human Rights (ECHR). In particular mass surveillance or 'bulk interception' by the Intelligence Services under section 8(4) RIPA and accompanying bulk intelligence-sharing which was revealed by Edward Snowden and confirmed in a report by the Intelligence and Security Committee ('the ISC report') published during the consultation period.[1] Liberty, along with Privacy International, Amnesty International, the American Civil Liberties Union and other human rights organisations is shortly due to lodge an application at the European Court of Human Rights in Strasbourg challenging the Part 1 regime.

3. In this response we concentrate on provisions and changes to the Draft Code that are of greatest concern to Liberty. The amendments largely comprise anodyne repetitions of the language of proportionality and explanations of woefully weak systems of internal review, record keeping and the self-application of broad and ill-defined standards. The revised code offers no substantive movement towards a more targeted and human rights compliant approach to surveillance. Where it does reflect substantive changes to the law, these are retrograde in nature, expanding the already vast surveillance capacity of the state.

4. The Draft Code is also noteworthy for its substantial omissions. It is largely silent on the issue of intelligence sharing with the UK's intelligence partners, a disturbing omission given the admission of the General Michael Hayden, former director of NSA and the CIA, that *"we kill people based on metadata".*[2] Liberty has had sight of the response by the APPG on Drones to the present consultation

[1] The Intelligence and Security Committee, *'Privacy and Security: A modern and transparent legal framework'*, 12 March 2015.
[2] See http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata.

exercise which identifies, as a primary concern with the Code, its failure to properly address the sharing and end-use of intercepted data by a foreign state.[3] Liberty shares the concerns of the APPG, which are particularly compelling given the use to which intercepted data may be put once shared with foreign powers, including the facilitation of lethal drone strikes on foreign soil.

Extra-territoriality

5. Paragraph 2.6 of the Existing Code specifies that interception warrants cannot be served on those outside the jurisdiction of the UK. Paragraph 3.8 of the Draft Code states that a warrant "*may be served on any person who is required to provide assistance in relation to that warrant*" and paragraph 3.9 extends the duty on CSPs to implement warrants to "*any company offering services to customers in the UK, irrespective of where the company is based*". This major change reflects provisions introduced in the Data Retention and Investigatory Powers Act 2014 (DRIPA) to give RIPA extra-territorial effect. During the passage of that "emergency" Bill, the Government maintained it had always understood RIPA to have extra-territorial effect. This change to the interception code confirms the accuracy of Liberty's position, that hitherto RIPA had not had extra-territorial effect. Parliament was badly misled by Government on this point.

6. RIPA places a requirement on CSPs to take all reasonably practicable steps to give effect to the warrant as are notified to them. However following DRIPA's amendments to RIPA, paragraph 3.11 of the Draft Code states ''*When considering this test, section 11(5)(a) specifies that regard must be had to any requirements or restrictions under the law of the country where the CSP is based that are relevant to the taking of those steps. It also makes clear the expectation that CSPs will seek to find ways to comply without giving rise to conflict of laws. What is reasonably practicable should be agreed after consultation between the CSP and the Government. If no agreement can be reached it will be for the Secretary of State to decide whether to press forward with civil proceedings. Criminal proceedings may also be instituted by, or with the consent of, the Director of Public Prosecutions."*

7. This addition simply serves to emphasise the impossible situation that CSPs will be placed in when the UK Government makes demands that would require them to breach the laws of their host State. Due to RIPA's expansive powers, the

[3] Submission of the APPG on Drones to the Consultation on the Draft Code of Conduct on the Interception of Communications.

Secretary of State could, for example, serve Gmail with an 8(4) warrant in California, USA, requiring it to intercept all communications between subscribers in two specified countries. The Draft Code confirms that attempts will be made to force companies to provide assistance within the lax and expansive legal framework set out under RIPA.

8. When extra-territorial provisions were proposed in the Draft Communications Data Bill, the Committee reported that -

> *"All the overseas CSPs which gave evidence to us had major concerns about the jurisdictional issues, and in particular about overlapping jurisdiction. Stephen Collins from Hotmail said that the Home Office had not explained how it would address the possibility of obligations in the draft Bill putting Microsoft in a position of legal conflict with its home state laws in the USA, Ireland and Luxembourg. Emma Ashcroft from Yahoo! was concerned that extending jurisdiction would set a "global precedent" with the United Kingdom being the first State to adopt provisions of this type. She believed that other States would follow, using legislation to limit free expression and infringe privacy rights. She felt that the draft Bill "would create a bewilderingly complex patchwork of overlapping and potentially conflicting laws, and put companies like ours in a very difficult position where we have to make difficult decisions about how to be consistent in our approach to law enforcement and protecting our users." Colin Crowell from Twitter said that there were questions about the assertion of authority over a company subject to US laws…Simon Milner told us that Facebook would "strongly oppose" a measure requiring it to violate the law of another State."*[4]

9. The alternative, most appropriate, and probably most successful way for Government to seek to access information held overseas is to extend and improve the use of Mutual Legal Assistance Agreements (MLATs) with other States. MLATs operate under the *Crime (International Co-Operation) Act 2003* and provide a legal basis for information sharing between States for the purposes of detecting and prosecuting crime. They provide a transparent framework, avoiding the legal complexities and human rights risks of States seeking to act unilaterally, leaving service providers as the only barrier against privacy violations. Not only do they offer the best way of ensuring that safeguards are applied internationally, but they have

[4] Report of the Joint Committee on the Draft Communications Data Bill, November 2012, paragraph 239-40.

the capacity to be an extremely effective method for the transfer of information. The Government has claimed that the MLAT system is too slow and bureaucratic to be an effective tool. However MLATs are wholly a product of Government – the terms are decided by Government, they are implemented by Government and they are funded by Government. It is difficult to see why, with commitment and leadership, inefficiencies cannot be reduced and MLATs turned into a useful, human rights compliant model for information sharing between states.

Duration of Interception Warrants

10. The Existing Code states that all interception warrants are valid for an initial period of three months (but may subsequently be renewed, in the case of national security/ economic wellbeing of the UK grounds for a further six months, otherwise for a further three month period).[5] By contrast the Draft Code states that interception warrants issued on serious crime grounds are valid for an initial period of three months, but that interception warrants issue on national security/economic wellbeing of the UK grounds are valid for an initial period of six months.[6] No policy argument has been advanced as to why the initial duration for interception warrants related to those grounds should be doubled. This is a significant extension of power that runs wholly counter to the widespread public and parliamentary concern over the bulk interception practices currently undertaken by the Intelligence Agencies. The only other change is a perfunctory reference to the fact that proportionality should be a matter for consideration where a recommendation is made to the Secretary of State that an existing warrant be cancelled. The decision remains in the hands of the Secretary of Secretary.

Provision of permanent interception capability

11. Under the Existing Code, persons who provide a public postal or telecommunications service may be required to provide a "reasonable interception capability". Under paragraph 3.13 of the Draft Code, such persons may be required to provide a "permanent interception capability" – testimony to the scale of the ambitions of Government and the Agencies. Again this is a sweeping extension of Executive power that has not been accompanied by explanation or justification. It seemingly institutionalises permanent interception capabilities – including mass interception capabilities – and when combined with the new DRIPA power to

[5] Paragraph 2.11 of the Existing Code.
[6] Paragraph 3.17 of the Draft Code.

mandate interception by CSPs outside the UK represents a breath-taking expansion of the State's surveillance capacity.

Additional information on safeguards that exist in relation to section 8(4) RIPA

12. As the consultation document acknowledges "*interception is among the most intrusive powers available to law enforcement and the security agencies."*[7] Liberty remains convinced that the statutory framework under 8(4) which allows bulk interception of 'external communications' is not compliant with the ECHR. According to the ISC report, 19 warrants are currently in operation authorising the external interception of all communications carried by a specific named CSP and a further warrant which covers GCHQ's own interception operations.[8] Certificates are supposed to restrict which communications can be examined, however the ISC describes these as "*so generic, it begs the question as to whether it need be secret*".[9] Section 8(4) is also interpreted as allowing the interception of communications not identified in the warrant whose interception is necessary in order to do what the warrant authorises.[10]

13. External communications are defined as communications either sent or received outside the UK or both. Internet based communications have eradicated the distinction between external and internal communications. External communications include browsing websites located overseas, anything posted on a social media site overseas, overseas cloud storage and the use of overseas email provider such as Hotmail or Gmail. While the communications of people known to be in the UK cannot be searched, it is likely that for the vast majority of bulk interceptions, the Agencies have no knowledge of where the individuals are located. The ISC took oral evidence from the Foreign Secretary regarding 'external' interception and said that his answers "*appeared to indicate that all internet communications would be treated as external communications under RIPA – apart from the increasingly tiny proportion that are between people in the UK, using devices or services based only in the UK, and which only travel across network infrastructure in the UK*".[11] The Committee concluded that the current system "*is confusing and lacks transparency*" and that "*Government must*

[7] Home Office Consultation: Equipment Interference and Interception of Communications Code of Practice, page 4.
[8] ISC report, finding N, page 39.
[9] Ibid, paragraph 101.
[10] Annual Report of the Interception of Communications Commissioner, 2014, para 6.25.
[11] ISC report, paragraph 109.

publish an explanation of which internet communications fall under which category and ensure that this includes a clear and comprehensive list of communications".[12]

14. The legislative reform urgently required could not be delivered in a Code of Practice. The proposed changes to the Code, however, simply explain the bewildering extent of the licence for mass-interception - without any requirement to specify or define the subject - under section 8(4).

15. The Draft Code places beyond doubt the fact that these vast interception operations are not conducted as part of an ongoing investigation into criminal activity, but rather an effort to create a what was described in a recent and highly critical report by the European Parliament as a *"fully-fledged preventive state"* unrestrained by national borders.[13] Liberty supports the European Parliament's observation that it "*strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society*"[14]

16. The Draft Code offers some basic explanation of other deeply unsatisfactory elements of the system of mass, executive-led warrantry, including the process of data-mining of information collected under section 8(4), which facilitates access to information subject only to reliance on one of the broad purposes set out in an accompanying certificate.[15] The Code sketches out the weak and patchy safeguards which apply to the system operated under section 8(4), including internal scrutiny and retrospective review by the Interception of Communications Commissioner. The Draft Code includes a description of the inadequate and perfunctory safeguards applicable to section 8(4) warrants under section 16 of RIPA, including a structure of internal guidance, self-regulation and internal record keeping liable to provide little or no protection against institutional expansion and abuse of already unfathomably broad capabilities.[16]

---

[12] Ibid, Finding O.
[13] European Parliament Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, published 21 February 2014, paragraph 5, available at - http://www.polcms.europarl.europa.eu/cmsdata/upload/73108fba-bb11-4a0b-83b8-54cc99c683b5/att_20140306ATT80632-1522917198300865812.pdf.
[14] Ibid, paragraph 12.
[15] Draft Interception of Communications Code of Conduct, section 6(4).
[16] Draft Interception of Communications Code of Practice, paras 7.10 – 7.19.

Privileged and confidential information

17. According to the Consultation document, the Draft Code now makes explicit the *"robust safeguards"* that prevent the misuse of confidential information. The Code includes significantly more detail than the Existing Code on the internal policies which exist around the interception, either deliberately or incidentally – of legally privileged information. There are a number of ways in which the Agencies may acquire legally privileged information: deliberate interception of lawyer-client communications; targeted interception of solicitors; bulk interception of 'external communications' or intelligence sharing; or as a result of an "IT operation" under sections 5 or 7 of the *Intelligence Services Act 1994*.

18. Concerns around interception of this particularly sensitive information were thrown into sharp focus by a recent disclosure in the *Belhaj* litigation concerning two victims of an SIS-CIA rendition and torture operation. In the course of proceedings before the Investigatory Powers Tribunal in October 2014, the Government conceded for the first time that the Intelligence Services had policies relating to the interception of private calls between lawyers and their clients. They refused, however to give further information at that stage, on the grounds that the information might *"be damaging to public interest or prejudicial to national security"*[17]. On 15 February 2015, the Government further conceded that "*since January 2010 the policies and procedures for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material have not been in accordance with human rights legislation specifically Article 8(2) of the ECHR."*[18]

19. In evidence to the ISC in 2014, SIS maintained that applications for warrants which may involve intercepting legally privileged information are only made in "*exceptional and compelling circumstances*".[19] The Committee reported cryptically that "*SIS are more likely to obtain sensitive information through their acquisition of Bulk Personal Datasets".*[20] The existence of Bulk Personal Datasets was revealed for the first time in the ISC report. Very little is known about them, save that they "*vary in size from hundreds to millions of records*" and that they "*may include significant*

[17] For more see: http://www.reprieve.org.uk/case-study/abdul-hakim-belhaj/.
[18] "Government concedes policies on lawyer-client snooping were unlawful", Reprieve, 15 February 2015, available at - http://www.reprieve.org.uk/press/government-concedes-polices-on-lawyer-client-snooping-were-unlawful/
[19] ISC Report, paragraph 258.
[20] ISC Report, paragraph 258.

quantities of personal information about British citizens."[21] None of the Agencies are able to provide statistics about the volume of personal information about British citizens that are included in BPDs. Those that contain legally privileged information, medical information or journalistic information apparently require *"a higher degree of justification for retention and exploitation".*[22]

20. With regard to legally privileged material obtained by the Agencies which is relevant to court proceedings in which the Government has an interest, GCHQ claim to implement *"Chinese wall arrangements…. To ensure no cross contamination of…intelligence information to lawyers or policy staff who might be involved in….litigation".*[23] MI5 has guidance to ensure that where legally privileged material is obtained *"MI5 legal advisers do not become aware of the content of legally privileged material that may be relevant to proceedings [against MI5] in which they are instructing [directly] counsel and in which MI5 has a direct interest in the outcome."*[24] SIS claims to have "*a detailed policy…governing the potential interception of communications relating to litigation, other legal proceedings or criminal investigations in which SIS or HMG may be a party to or have an interest in".*[25]

21. The further detail provided in the Draft Code seems to be, at least in part, a response to the Court proceedings that have forced revelations about the interception. The explanatory information given in the Code of Practice offers little reassurance. It confirms that the Secretary may issue a warrant providing expressly for the interception of legally privileged information where she believes there are exceptional and compelling circumstances and reasonably regards interception as likely to yield intelligence necessary to counter a threat to, for example, national security. It is for the Secretary of State to make an assessment of proportionality in these circumstances. She may, but need not, impose additional conditions for interception, such as reporting requirements to allow her to review the process. Legally privileged information can be disseminated where this is judged lawful by a Home Office legal advisor, subject only to a warning that it is privileged. The Code states that privileged information should not be allowed to directly fall into the hands of the prosecuting authorities, where the information is connecting to a prosecution they are conducting. There is no parallel restriction on disclosure of information to

[21] ISC report, paragraph 158.
[22] ISC report, paragraph 258.
[23] ISC report, paragraph 259.
[24] ISC report, paragraph 260.
[25] ISC report, paragraph 261.

law enforcement authorities, and no restriction on their conveyancing the substance of that information to prosecutors. In civil proceedings public authorities may not "rely" on intercepted, privileged information to gain a litigation advantage over their opponents, but there is no apparent prohibition on the public authority or their lawyers having sight of such information. The Code states that the Interception of Communications Commissioners should be notified of interception of privileged information in order that he can retrospectively consider whether the power has been exercised in accordance with the above guidance. The explanation provided as to the treatment of legally privileged information in the Code gives a disturbing picture of current practice, reveals the lack of substantive safeguards and makes a nonsense of the whole concept of legal professional privilege.

22. The Code also details the treatment of confidential, journalistic communications and sensitive communications between MPs and their constituents.[26] The relevant sections of the Code offer no substantive protection, simply stipulating that interception is permissible where the Home Secretary judges it necessary and proportionate in pursuit of one of a series of broad purposes. Further dissemination is permitted subject only to the caveat that reasonable steps be taken to mark the information out as confidential.[27] Where there is doubt surrounding further dissemination, legal advice is to be sought. Rather than setting minds at rest the present Code will be a disturbing read for journalists and politicians, whose confidential communications are, in reality, treated with a similar disrespect to those of the broader population.

[26] Draft Code, paras 4.21-4.24.
[27] Draft Code, para 4.23.