GMG submission to ISC enquiry into privacy & security

Introduction

1. Guardian Media Group (GMG) is pleased to respond to the Intelligence & Security Committee's (ISC) enquiry into the balance between privacy and security. GMG is the publisher of the Guardian newspaper, associated Guardian applications and website, and a range of other businesses for whom digital technology is vital for its present and future economic prosperity.
2. GMG's future is wedded to the growth of the UK digital economy, and to the enabling power of the internet to access new markets across the globe. As we near the 25th anniversary of the British creation of the World Wide Web, it is important that the UK leads the long term debate about securing an open and secure internet in word and deed, to ensure that individuals and businesses can have faith, confidence and trust in the online world.
3. While the primary focus of debate about the Snowden revelations has been a binary debate between the competing public interests of privacy and security, the reporting of the Snowden files by the Guardian and many other newspapers across the world illuminate a range of other public interest considerations that the ISC should weigh in the round in order for this enquiry to have suitable credibility. These include the consequences of agency programmes that have:
    a. **Risked the integrity of the web itself** through the weakening of encryption protocols used by businesses and consumers through the insertion of backdoors[1];
    b. **Undermined legal privilege in commercial and criminal cases**[2] and put at risk the confidentiality of journalistic sources and material;
    c. **Risked the future of the digital economy,** with one Washington-based foundation predicting a potential economic loss to the US cloud computing industry alone of as much as $35 billion over the next 3 years through to 2016[3];

[1] Revealed: how US and UK spy agencies defeat internet privacy and security http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[2] Complaint filed over UK spying on Libyan torture victims' legal communications http://www.reprieve.org.uk/press/2013_10_14_PUB_UK_spying_libyan_torture_victims/
3 http://www2.itif.org/2013-cloud-computing-costs.pdf

d. **Undermined the moral weight** of public statements made by UK and US leaders about the importance of an open internet[4];
e. **Made a mockery of the concept of Parliamentary sovereignty**, by circumventing the twice-stated-will of Parliament to reject Government calls for the capability to bulk collect the digital communications of British citizens.

4. In weighing these public interests, GMG absolutely recognises that there are aspects of the workings of the intelligence agencies that must remain secret. GMG also recognizes the difficulty of debating the previously secret activities of organs of the State in public. However, as President Obama said last year *"What makes us different from other countries is not simply our ability to secure our nation… It's the way we do it, with open debate and democratic process."*[5]
5. In the absence of such political leadership in the UK, this enquiry represents both a huge opportunity, and a huge test for the ISC to demonstrate to the British public that it can balance arguments across the full range of public interests at play in this debate. Time after time in recent years, whether in relation to the rendition of UK citizens, or the torture of citizens in Libya[6], the ISC has failed to hold the UK intelligence services to account on behalf of Parliament and the British people. It is unsustainable that it should fall to journalists, courageous backbench MPs and NGOs to hold the intelligence agencies to account, especially – as this submission details later on – if the very programmes that form the centre of this debate potentially undermine the confidentially of journalistic sources and material.
6. Following the publication of the Snowden revelations, the contrast between the debate in the UK and the United States is stark. In the US there is a deep

---

[4] *"The WAN-IFRA membership is deeply concerned by the British authorities' treatment of the profession of journalism and its attempts to control the public debate.*
"The British government's actions have far reaching consequences across the globe - particularly within the Commonwealth - and any threats to the independence of journalism in Britain could be used by repressive regimes worldwide to justify their own controls over the press.
http://www.wan-ifra.org/press-releases/2014/01/15/global-press-freedoms-organisations-begin-press-freedom-mission-to-the-uni

5 http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/09/edward-snowden-patriot/

6 http://www.newstatesman.com/politics/2013/12/intelligence-and-security-committee-governments-white-washing-body-choice

and robust debate about the balance between privacy and security, leading to sweeping Presidential reforms. Contrast the findings of the Privacy and Civil Liberties Oversight Board, an independent liberties advocate in the executive branch, with the unchallenged assertions of the heads of UK intelligence services about the efficacy of these intelligence programmes in their first public appearance in front of the ISC on 7th November 2013.

7. In the United States we have seen the media, the general public, policy makers and the President address what is and will remain one of the most important challenges of our lifetimes – the limits of state power over our digital lives. The debate has been open, transparent and honest, most recently on 23rd January 2014 with devastating findings of agency overreach by the President's own Privacy Oversight Board[7]. This approach has led to wide-reaching Presidential reviews, a range of bi-partisan Acts in Congress, cases brought before the courts challenging the legality of the practices of the NSA, and a series of reforms announced by the White House. It is now time for the UK Parliament to reassert its control over agencies and programmes operating at the very edges of laws created for a different era.
8. In the remainder of this document, GMG outlines:
    a. Why RIPA 2000 is an inappropriate framework to govern intelligence agency activity in a radically-changed digital world;
    b. Why the distinction between 'content' and 'metadata' is artificial, raising questions about the lax oversight in relation to the capture and analysis of metadata;
    c. Concerns about the inadequate regulation of extraterritorial data transfers;
    d. Specific concerns about the inadequacy of the public oversight and transparency framework in which the agencies operate;
    e. The case for the use of intercept evidence in court;
    f. Concerns about the use of mass interception on privileged journalistic material.

[7] http://www.theguardian.com/world/2014/jan/23/nsa-barack-obama-phone-data-collection-illegal-privacy-board

Interception in a digital world

9. The argument made and lost by the previous Labour and, more recently, Coalition Government, that the law enforcement and the intelligence services in the UK need new powers in order to 'maintain the capability' of the State in a digital age falls down on two counts:
    a. First, far from maintaining the capabilities of the security services, the Intercept Modernisation Program, then through the Communications Capabilities Development Programme (CCDP) and the proposed Data Communications Bill, aimed to capture, store and analyse vast amounts of private communications on a scale that would have been inconceivable in a pre-digital age. Programmes like Tempora – revealed to the public and to the ISC in the Guardian - enable the intelligence services to intercept vast amounts of data stored or shared using modern electronic communications systems, by placing data interceptors on transatlantic internet cables.[8] The fact that the UK is a key landing point for transatlantic subsea cables enables the intelligence services to access a very substantial proportion of global internet traffic.
    b. Second, the importance of digital communications technology and platforms to the lives of consumers has increased dramatically between 2000 and 2014. In just one of the programmes identified in the Snowden files, GCHQ is estimated to handle in the region of 600 million "telephone events each day".[9] This is not to mention the enormous volume of personal information held on social networking sites such as Facebook by online retailers, banks and others.
10. The combination of the cheap electronic storage of vast amounts of citizen data with hugely powerful datamining and link analysis programmes provides intelligence agencies with huge insight into the behaviour of groups

[8] The Guardian has reported that "by the summer of 2011, GCHQ had probes attached to more than 200 internet links, each carrying data at 10 gigabits a second" and that this mode of surveillance potentially gives GCHQ access to 21 petabytes of data a day. A petabyte is approximately 1000 terabytes (which is in turn 1000 gigabytes). This quantity of data is equivalent to sending all the information in all the books in the British Library 192 times every 24 hours, "GCHQ Taps Fibre-optic Cables for Secret Access to World' s Communications", The Guardian, 21 June 2013.

[9] *Ibid*.

and individuals. Sophisticated computing can identify embedded patterns and relationships, including personal information, habits, and behaviour. Individual pieces of data that previously carried little potential to expose private information may now, through datamining and link analysis, reveal sensitive personal, privileged or professional information pertaining to individuals and organisations. This is of particular concern in the context of journalism, where the confidentiality of contacts and journalistic sources are of vital importance.

11. Following Parliament's refusal to pass either the Intercept Modernisation Programme or the Draft Communications Bill, these intelligence agency capabilities have been shoehorned within the existing provisions of RIPA 2000, raising huge questions about their legal basis as a consequence.

Section 8 (4) of RIPA 2000

12. A key problem with the present legislative framework for the interception and collation of data concerns the inadequate and outdated regulation of the collation of "external communications", which encompasses gargantuan quantities of personal, professional and privileged data pertaining to UK nationals and residents as well as businesses operating in the fields of commerce, law, media (including journalism) and industry. Section 8 (4) of RIPA 2000 removes the requirement, in respect of the interception of "external communications", that a warrant providing authorisation for interception must specify a particular person or "set of premises" to be made subject to interception. Moreover, as long as authorisation is provided by the Secretary of State, Section 8 (4) merely requires the warrant to provide the descriptions of "intercepted material the examination of which [the Secretary of State] considers necessary" in the interests of "national security", "preventing or detecting serious crime", or "safeguarding the economic well-being of the United Kingdom".[10]

[10] Section 8 (4), RIPA 2000.

13. As a result, "external communications",[11] defined as a "communication sent or received outside the British Islands" (which will include the huge range of data stored on servers located outside the United Kingdom) can be intercepted on a more imprecise basis than other communications. In practice, GMG understands from external legal counsel that Section 8 (4) warrants authorise the interception of generic and vaguely-described forms of material and are renewed on a six monthly basis (so are in place, in effect, indefinitely).
14. Parliament could not have envisaged either (i) the exponential growth in capacity for the collation and processing of information on a gargantuan scale; or (ii) crucially, the extent to which, through social networking and other online facilities, vast quantities of personal, privileged and professional data would be stored and communicated online. The legislative framework is therefore outdated.
15. Furthermore, from a legal perspective, it is very doubtful whether this scheme complies with the requirements of Article 8, ECtHR.[12] It is well-established that the collation and storage of information by State authorities on individuals amounts to an interference with the right to a private and family life which must satisfy the requirements of Article 8.[13] In particular any interference must be "in accordance with law" (in particular satisfy the need for legal certainty and foreseeability), and must manifest sufficient safeguards against arbitrariness and satisfy the criterion of proportionality. In relation to practices under Section 8 (4), key problems include:
    a. No meaningful assessment of proportionality of interference can be undertaken at the level of generality at which generic interception warrants are granted;

---

11 *See* Section 8 (5), RIPA 2000.

12 Note that *Kennedy v. the United Kingdom*, which found that aspects of the interception regime set out in RIPA 2000, was not concerned with the regime concerning "external communincations". *See Kennedy v. the United Kingdom* 52 EHRR 4 (2011).

13 This was confirmed recently by the Court of Appeal in *R. (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2013] 1 W.L.R. 3305. It is a position established by the ECtHR in a series of cases e.g. *Segerstedt-Wiberg v Sweden* (2006) 44 EHRR 14. In the context of the EU Charter of Fundamental Rights, see the recent decision of the Advocate General of the CJEU in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* Case C-293/12 finding that EU directive 2006/24/EC that requires telecoms and internet providers to store data on phone and email traffic for two years is a "serious interference" with citizens' right to privacy.

b. It appears that, in practice, permission for generic authorisation warrants are granted on a rolling basis and in place indefinitely;
c. As regards foreseeability and arbitrariness, the circumstances in which an individual or group's communications may be intercepted, retained and processed is wholly unclear. Indeed, the existence of the programmes had not even been formally acknowledged before the Guardian's reporting.
d. The degree of intrusion authorised through the generic warrants is considerable, justified by reference to broad, abstract notions of "national security", "the prevention of serious crime" or the economic welfare of the United Kingdom.

Reform required

16. GMG agrees with the proposal of the Parliamentary Joint Committee of Human Rights that "RIPA 2000 be amended to provide for judicial rather than ministerial authorisation of interceptions, or subsequent judicial authorisation, in urgent cases".[14] GMG submits that this approach should be applied both to the authorisation of communications internal to the United Kingdom and for "external communications".
17. The present system offers insufficient safeguards of independence in the authorisation process. Secretaries of State, who are responsible under RIPA for the issuing of sweeping, generic "certificates" for the interception of "external communications", are asked to authorise interception by agencies for which they are ultimately responsible. Government departments are often under enormous political pressure, whether from foreign governments for cooperation, from the public to respond decisively in the fight against terrorism and other serious crime, or to protect jobs and promote economic welfare. The risk that overbroad or intrusive authorisations may be granted in pursuit of these goals, influenced by these political pressures, is great. Politicians, much less ministers, can hardly be expected to be immune from

[14] Joint Committee on Human Rights, Counter-Terrorism and Human Rights: 28 Days, Intercept and Post Charge Questioning, (HL 157/HC 394), 30 July 2007, at 161.

the pressure of politics and public opinion. Real concerns therefore exist as regards whether authorisation by the SSHD provides sufficient independence and serves as an effective safeguard for privacy.

18. This is born out in practice. Although figures are not publicly available it has been acknowledged by successive Interception Commissioners that the refusal of a warrant by a Secretary of State "is rare".[15] This has, it appears, been the case for many years. Real doubts therefore exist as to whether the authorisation process serves to provide meaningful scrutiny of requests.

19. Judges or, at the very least, persons independent of political pressures offer the best safeguards of independence and impartiality. This is all the more important given that interception decisions are necessarily made in secret when affected persons have no opportunity to seek to protect their own interests. As the ECtHR held in *Klass v. Germany*:

    a. *The rule of law implies … that an interference by executive authorities with an individual's rights should be subject to effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and proper procedure.*[16]

20. Furthermore, a system of judicial authorisation is eminently workable - indeed, is perhaps preferable on grounds of efficiency to the system presently in place. In this regard, the following points should be noted:

    a. Precisely this system operates successfully in many European states and in many democracies in other regions of the world;[17]

    b. High Court judges are very experienced in dealing with very complex matters, on an urgent or very urgent basis, and deal with requests for urgent relief often within a matter of hours if necessary (including out of hours and at weekends or on public holidays);

---

15 *See e.g.* Report of the Interception of Communications Commissioner for 2003, July 2004, at 8 and, to similar effect, Report of the Interception of Communications Commissioner for 2009, at 2.3; and Report of the Interception of Communications Commissioner for 2010, at 2.4.

16 *Klass v. Germany*, 2 E.H.R.R. 214 (1980). *See also Popescu v. Romania* (No. 2), Merits, 26 April 2007, Application No. 71525/01 at 70-73 and *Lordachi v. Romania*, 10 February 2009, 25198/02, at 40, where the Court held "the body issuing the authorisations for interception should be independent … and there must be judicial control or control by an independent body over the issuing body's activity".

17 See *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime*, United Nations Office of Drugs and Crime, available at: http://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

c. A High Court judge is likely, by virtue of his or her professional experience and background, to be better equipped to deal with the issues at stake (in particular weighing up the different legal interests) speedily and effectively than a Secretary of State, relying on the assistance and advice of his or her officials. The Secretary of State may well consider the matter diligently but has no necessary experience of acting in a judicial or quasi-judicial capacity, weighing different, often competing legal interests and considering matters such as the proportionality of interference;

d. Needless to say, a judicial authorisation process could be conducted *ex parte* and need not involve court proceedings or the formality of such proceedings.

21. In short, a process of prior judicial, rather than executive authorisation, would undoubtedly be effective in practice. It would offer greater guarantees for the rule of law, provide more independence and offer much greater reassurance that the legal framework in place, including the public's right to privacy, is respected.

The significance of Metadata

22. As a recent Guardian infographic demonstrates, the volume and variety of insight that metadata[18] generated by commonly-used digital services is significant. The privacy impact of collecting all communications metadata about a person or organisation over time (and aggregating and link analysing this data) is often vastly greater than the impact of collecting specific content data about a single person, group or organisation. There is no sufficient justification for the less rigorous and less independent regulatory regime applied in the context of metadata than that in relation to content.

23. Interception of content is authorised by the Secretary of State for three or six months (depending on the purpose) by a warrant specifying an individual or premises under Part I Chapter 1 of the Regulation of Investigatory Powers

[18] Metadata describes the characteristics of information or a communication, other than its content.

Act 2000. Interception of "communications data",[19] however, is regulated by the less rigorous regime set out in Part I Chapter 2 of RIPA.

a. First, the grounds on which communications data may be intercepted are much more expansive than those relating to content, including public safety, public health as well as the economic well-being of the UK, national security or the prevention and detention of crime (not just serious crime).[20]
b. Second, crucially, rather than authorisation being required by the Secretary of State,[21] a very wide range of "designated officials" in many different government departments and agencies may authorise persons in their agency to undertake the interception of metadata (in effect, a system of self-authorisation by various departments and agencies).[22]

24. The notion, oft repeated by Ministers and security officials, that metadata is less intrusive or meaningful than content is based on the discredited idea that metadata merely reveals matters such as the timings of particular emails or the location of computers used. Using new "dataveillance" and information synthesis technology, the collation of metadata now enables the exploitation of metadata in ways unimaginable at the time RIPA 2000 was enacted by Parliament, giving rise to substantial concerns about the collation of very sensitive, personal, professional or privileged information about individuals, groups, political parties, NGOs, media organisations, journalistic networks and their sources, lawyers and their clients, to give just a few examples.

Reform required

25. Where metadata is collated and exploited using information synthesis techniques, given that it poses as great a risk to individual privacy as content interception, it must be subject to the same regulatory regime, including

---

19 "Communications data" is defined, *inter alia*, as "any information which includes none of the contents of a communication [...] and is about the use made by any person–(i) of any postal service or telecommunications service; or (ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system". It is therefore to be distinguished from the content of communications.

20 Section 22 (2), RIPA 2000.

21 Section 5 (1), RIPA 2000.

22 Section 22 (3), RIPA 2000.

appropriate independent authorisation. The present system for the authorisation of the interception of metadata by numerous "designated persons"[23] who work for the organisations which seek to intercept such data is unsustainable.

Insufficient Regulation of Extraterritorial Data Transfer

26. The present regulatory system fails to provide sufficient protection in respect of the growth of the extraterritorial transfer of collated data, again a phenomenon the nature and scale of which was not contemplated at the time RIPA 2000 was enacted. A number of points are important in this regard.
    a. First, the powers of the NSA and other US agencies to intercept communications data of non-US persons outside the United States (including UK residents) are considerable and subject to few safeguards. The power is set out in Section 1881 (a) of the US Foreign Intelligence and Surveillance Act 1978 and permits "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information".[24] There is no requirement that the surveillance need be proportionate, nor even that it be necessary to protect specific interests such as national security. The US National Security Agency, it is understood, has direct access to data collected through the Tempora system[25]. In consequence it may, under US law, use such data in circumstances or in a manner that would not satisfy the requirements of domestic UK law or the European Convention on Human Rights (particularly where such data

---

23 *See* Section 22 RIPA 2000.

24 The definition of "foreign intelligence information" is set out in s 1801. It is very broad. Pursuant to section 1801(e) "foreign intelligence information" includes "information with respect to a foreign power or foreign territory that relates to ... the conduct of the foreign affairs of the United States." The term "foreign power" is defined in section 1801(a) to include not only foreign governments or entities directed or controlled by foreign governments, but also pursuant to section 1801(a)(5) "a foreign-based political organisation, not substantially composed of United States persons." Foreign-intelligence information thus covers information with respect to any foreign-based political organisation or government that relates to the foreign affairs of the US. It would thus, for example, include the contents of private and lawful discussions by those who are members of, or are communicating with, political organisations or governments that in any way relates to US foreign policy.

25 GCHQ has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process cast streams of sensitive personal information which it is sharing with the NSA in the United States. GCHQ taps fibre-optic cables for secret access to world's communications

concerns persons who are not US nationals or resident in the United States).

b. Second, limits on the use of data transferred to the United States are not publicly disclosed but are contained in the provisions of confidential agreements concluded between the United States and the United Kingdom. The United Kingdom is under an obligation not merely to refrain itself from arbitrary interference with the right to private and family life through the interception, retention and/or use of private information but is also, by virtue of the settled case law of the ECtHR, under a positive obligation to protect the right to private and family life from arbitrary interference by others. In *KU v. Finland*,[26] for instance, the ECtHR found violation where the State had failed to take "practical and effective" measures to protect the applicant's private life.[27] Given the scale of data collected through programmes like Tempora and the extent to which such data is transferred or made available to United States agencies, it is open to serious doubt whether the transfer and/or access is, given the limited safeguards in place, legal under United States law. These concerns are heightened given that the statute code of practice, prepared pursuant to Section 71, RIPA 2000, *Acquisition and Disclosure of Communications Data: Code of Practice*, expressly envisages situations where data is disclosed to other states "even though that country does not have adequate safeguards in place to protect the data".[28] Again, it is very doubtful whether such a practice is compatible with the requirements of Article 8, ECtHR.

Reform required

27. Under RIPA 2000 much depends on whether a communication may be described as an "external communication".[29] Crucially, where a

[26] *See e.g. KU v. Finland* 48 EHRR 52 (2009), at 42.
[27] *Ibid*. at 49.
[28] 7.21, *Acquisition and Disclosure of Communications Data: Code of Practice.*
[29] "External Communication" is defined in Section 20 RIPA as "a communication sent or received outside the British Islands". "Communication" is, in turn, defined in Section 81 (1) of RIPA as "(a) … anything transmitted

communication is "external", a special form of interception authorisation may be granted (a Section 8 (4) Certificate). This certificate, issued by the Secretary of State, need not specify a particular "set of premises" or "person" to be targeted (as is required in respect of the interception of other forms of content communication under RIPA 2000). A huge proportion of information stored or shared on the internet may be treated as "external" and therefore subject to this less rigorous regime, given that a great deal of information or data will be stored on servers outside the United Kingdom.[30]

28. Section 8 (4) certificates have, in practice, provided almost no check on the interception of all manner of external communication in recent years. In practice, the ten or so generic warrants which appear to be in place authorise the interception of an enormously broad range of generically described information, permitting interception on an almost blanket basis. Much greater precision in the certification process is required (not least to comply, it is submitted, with Article 8, ECtHR). Given the clear failure of the certification process to perform its function of providing precision and a safeguard against overbroad data interception, the level of precision required of a certificate should be legislatively prescribed.

29. It is accepted that there may be a justification, in certain limited circumstances, for large-scale surveillance in certain aspects of foreign relations. The intelligence services may, for instance, quite properly seek to engage in surveillance of certain oppressive foreign governments or criminal or terrorist organisations. Blanket surveillance of this nature should, however, be strictly scrutinised and authorised by way of specific warrants, identifying the foreign governments, foreign government entities, groups, organisations persons or entities targeted, to enable a meaningful consideration of the proportionality of interception.

30. In short, alongside the existing safeguards to the certification process set out in Section 16 RIPA 2000, more precise requirements as to the level of detail

---

by means of a postal service; (b) anything comprising speech, music, sounds, visual images or data of any description; and (c) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus".

[30] Note, however, that Section 16(1) and (2) RIPA 2000 provide that an interception warrant in respect of "external communications" may only be "referable to an individual" in the UK or "have as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him" if the Secretary of State certifies that this is necessary.

contained in a Section 8 (4) certificate should be specified in primary legislation. These requirements should bring to an end the practice of issuing generic warrants, at a very high level of abstraction, obviating meaningful or careful consideration of the proportionality and propriety of data interception.

Inadequate Public Oversight & Transparency

31. Present levels of public oversight and transparency are wholly inadequate. Through recent debates in Parliament it is clear that members of the ISC [31], and senior members of the Joint Committee that examined the Draft Data Communications Bill[32], were unaware of the existence of agency programmes reported by the Guardian.
32. Informed public debate about the many public interests involved in the interception of private information by the State should not be dependent on investigative journalism or whistleblowers. Available official guidance gives a wholly inadequate picture of the circumstances in which interception may take place.[33] Parliamentary debate, and the public more broadly, should be informed, at the very least, of the general nature of programmes in place and how such programmes are regulated in order to:
    a. **Protect legal accountability:** So that, if necessary, the question of whether a programme is lawful can be tested before the Courts, which is fundamental to the Rule of Law;
    b. **Protect against the arbitrary use of surveillance power:** By ensuring that categories of individuals, groups and organisations can understand the circumstances in which they may lawfully be made subject to the interception of data. Again this is fundamental to the Rule of Law;

31 http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm

32 http://www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance

33 See *Interception of Communications Code of Practice*, Seventh Impression 2007 and the *Acquisition and Disclosure of Communications Data Code of Practice*, First Impression 2007. It is entirely unclear from either of these documents that mass scale data interception has been authorised and is occurring. Indeed, the nature and scale of interception which is occurring is hard to reconcile with the statements of principle in the Codes of Practice. For instance, the Communications Data Code of Practice States that data interception will occur only when "necessary", "proportionate" and, "in accordance with law" (See 2.1, *Acquisition and Disclosure of Communications Data Code of Practice*).

c. **Ensure political and democratic accountability (and, if necessary, reform):** Given the ever-present speed of technological change in this area, the need for regulatory reform must be kept under continual review, which occurs in the context of a properly-informed public debate.

33. Without a properly-informed public debate, in which the nature of surveillance activities carried out are understood and the efficacy and propriety of the surveillance framework is the subject of continual review, the risk that the regulatory framework will become outmoded once more and that disproportionate surveillance methodologies will develop once again is considerable.

34. Given the fact that the ISC is the only Parliamentary Committee with any standing to hold the intelligence agencies to account, it is essential that through this enquiry, the public can be assured that the ISC is able has the powers, capabilities and resources to scrutinise the agencies activities. For example:

    a. Following annual evidence sessions, and sessions in relation to the draft Data Communications Bill, is the ISC satisfied it was provided with sufficient information about existing capabilities and programmes?
    b. Does the ISC have adequate resources and sufficient time to scrutinise the agencies' operations across the vast terrain it now roams on our behalf?
    c. Are new powers to request any document it wishes from the security services enough to hold the agencies to account in the absence of the broader context in which to analyse their significance?
    d. Do Members understand the extraordinarily complex and ever-evolving technology involved?
    e. Does the Committee have enough external assistance from technical experts that have not worked for the agencies or their contractors?
    f. Even after the reforms of the Justice and Security Act, is membership of the Committee sufficiently independent of Government?

g. Is it appropriate that Committee Members encumbered by decisions taken whilst a Minister with responsibility for agency activities should sit as Members of the ISC?

35. Alongside questions about oversight provided by the ISC, the ISC enquiry should consider the case for reform of the Investigatory Powers Tribunal (IPT). On the basis of information supplied by HM Courts Services, between 2001 and 2011 only 0.5 per cent of complaints were successful (6 cases out of 1,115). That is much less than figures for the same period before other tribunals and with no obvious reason why complaints made in a context marked by secrecy of decision-making would be substantially less meritorious.[34] Real concerns therefore exist as to whether the IPT provides an effective remedy in respect of unlawful interception. A number of substantial problems arise in respect of the IPT, its rules of procedure and, more generally, the fairness with which it operates:

    a. First, the degree of secrecy surrounding IPT proceedings.[35] In the recent Supreme Court case of *Bank Mellat v. Her Majesty's Treasury* (No. 1) [2013] UKSC 38, the Court reaffirmed that "[t]he idea of a court hearing evidence or argument in private is contrary to the principle of open justice, which is fundamental to the dispensation of justice in a modern, democratic society". An almost blanket rule of secrecy, such as that applied by the IPT, is inconsistent with the fundamental principle of open justice and undermines public confidence in the operation of the tribunal.

    b. Second, Section 67 (8) of RIPA 2000 provides an ouster of the jurisdiction of the High Court or, indeed, any other court to hear challenges to the decisions of the IPT.[36] The IPT cannot be assumed to be immune from errors of law or failures in fair

---

34 This compares to a success rate, in the same period of, for instance, 41% before the Immigration and Asylum Tribunal, 44% before the Criminal Injuries Compensation Tribunal, and 35 % in relation to tribunal cases concerning social security and child support. See *Freedom From Suspicion: Surveillance Reform for a Digital Age*, Justice October 2011.

35 Rule 9 (6), Investigatory Powers Tribunal Rules 2000. In *Kennedy v. G.C.H.Q* IPT/01/62, the IPT held that this provision, requiring all proceedings to be held in secret, was ultra vires. The rule, however, has not been amended and, in practice, hearings often proceed, even on matters of directions, without a claimant being notified of the hearing or provided opportunity to make submissions. All other rules were upheld by the IPT in Kennedy.

36 Section 67(8) of RIPA 2000 provides: "[e]xcept to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court."

procedure any more than another court. But this provision purports to prevent any such failure being challenged, which, in the event of a failure of fair procedure, likely violates Article 6, ECtHR.[37] This is all the more concerning since, under its rules, the tribunal cannot inform a party that a hearing has even been held (even on a matter such as directions) to enable submissions, even simply on issues of open justice or matters concerning the administration of a case, without the consent of the other party,[38] and a hearing will rarely be held *inter partes*. The scope for uncorrected errors of fact and law is therefore great.

Reform required

36. The efficacy of reforms made as a result of the passing of the Justice and Security Act (JSA) to strengthen the independence and resourcing of the ISC will take time to prove. However, in light of revelations that Members of the ISC were unaware of crucial agency programmes, calls made by Opposition Ministers during debates on the JSA that the ISC should become a full Select Committee of the House of Commons merit further consideration – not least because of the greater protection offered to witnesses and the potential penalties for misleading evidence provided to Select Committees.
37. There are substantial concerns regarding the fairness and efficacy of proceedings before the IPT and, given the statistics cited earlier, whether it provides an effective check on disproportionate or unlawful surveillance practices such as those reported by the Guardian. Fundamental revision of aspects of the IPT's operation is therefore required.

The use of intercept evidence in court

38. The UK is one of the very few countries which completely prohibits the use of intercept evidence in civil or criminal proceedings. GMG supports the view of

37 See e.g. *Kingsley v. the United Kingdom*, 35 EHRR 177 (2002).
38 IPT Rules 6 (2)- (4).

the *Privy Council Review Intercept as Evidence 2008*[39] that this prohibition should end.

39. Section 17 (1), RIPA provides that "no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of, or in connection with, any legal proceedings or Inquiries Act proceedings which (in any manner)– (a) discloses [...] any of the contents of an intercepted communication or any related communications data; or (b) tends ... to suggest that [interception had occurred or that a warrant for interception had been issued].

40. Most other countries regularly use intercept evidence in open court without any consequent loss of intercept capability, including other common law jurisdictions with similar criminal procedures and disclosure obligations to those which exist in the United Kingdom.[40] As the Prime Minister noted in a debate on the matter while in opposition in 2008, "'...*The Australian example, in particular, provides a number of interesting ideas for how the UK could attempt to derive benefit from intercept as evidence, whilst not unacceptably increasing the risk of disclosure to intelligence agencies and their sensitive capabilities and techniques."*[41]*.*

Reform required

41. GMG understands there is broad Parliamentary consensus on the need to use intercept evidence in court[42], and urges the Government to look again at how the prohibition set out in Section 17 (1) RIPA be ended.

---

39 *See Privy Council Review Intercept as Evidence : Report to the Prime Minister and Home Secretary*, 2008, p. 31 Cm 7324.

40 See Privy Council Review Intercept as Evidence : Report to the Prime Minister and Home Secretary, 2008, p. 31 Cm 7324.

41 http://toryspeeches.files.wordpress.com/2013/11/david-cameron-statement-on-the-use-of-intercept-evidence.pdf

42 http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140121/debtext/140121-0003.htm#140121-0003.htm_spnew86

Mass Interception and Privileged Journalistic Material

42. As outlined above, GMG is especially concerned about the lack of safeguards in place to prevent the mass interception and collation of data by the intelligence services undermining privileged journalistic material and the confidentiality of journalistic sources. The security of such material is absolutely vital to the journalistic function in a democratic society, including journalism which seeks to hold the State and its institutions (including the intelligence services) to account. As Lord Woolf held in *Ashworth Hospital Authority v MGN Ltd* [2002] UKHL 29 [at 61]:

> *[I]nformation which should be placed in the public domain is frequently made available to the press by individuals who would lack the courage to provide the information if they thought there was a risk of their identity being disclosed. The fact that journalists' sources can be reasonably confident that their identity will not be disclosed makes a significant contribution to the ability of the press to perform their role in society of making information available to the public.*

43. It is well established in the jurisprudence of the ECtHR that "freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance" (*Goodwin v. the United Kingdom* (1996) 22 E.H.R.R. 123, [at 39]).
44. Although the protection of journalistic sources is not absolute, it can only be abrogated where justified by "overriding requirement in the public interest" (a high threshold), with any restrictions subject to strict scrutiny by the Courts (*Goodwin v. the United Kingdom* (1996) 22 E.H.R.R. 123, [at 39-40]. GMG believes that a fundamental safeguard, in this context, is that the circumstances in which the confidentiality of journalistic material has been contravened must be "in accordance with law", meaning that the nature of any restriction must be clear, accessible and foreseeable.

Reform required

45. The mass interception of data and communications will *inevitably* result in journalistic material being intercepted and collated. However, whether there are presently any guidelines or safeguards in place as regards the handling of such material or its dissemination within government agencies (much less whether such safeguards are sufficient and lawful) is wholly unclear. In the absence of the publication of clear guidance and rules regulating and restricting the interception of journalistic material, particularly as regards the interception of "external communications", such a process can neither comply with the rule of law nor satisfy the requirement of legality under Article 10, ECtHR. At the very least, rigorous safeguards, which are clear and accessible to the public, are required.

Guardian Media Group
February 2014