Initial Assessment By The UK National Contact Point For The OECD Guidelines For Multinational Enterprises

COMPLAINT FROM AN NGO AGAINST 6 UK BASED TELECOMMUNICATION COMPANIES

JULY 2014

Contents

Summary of the UK NCP decision 3

The complaint 3

Responses from the companies 3

Guidelines provisions cited 7

The Initial Assessment process 9

Handling process 9

UK NCP decision 10

Identity of the complainant and their interest in the matter: 10

Whether the issue is material and substantiated: 10

Relevance of applicable law and procedures, including court rulings 13

How similar issues have been, or are being, treated in other domestic of international proceedings: 14

Whether the consideration of the specific issue would contribute to the purpose and effectiveness of the Guidelines 14

Next steps 14

Summary of the UK NCP decision

- **The UK National Contact Point (NCP) for the OECD Guidelines for Multinational Enterprises (the Guidelines) has decided to reject the complaint. This Initial Assessment concludes the complaint process under the Guidelines.**
- **This Initial Assessment was issued to the parties on 11th July 2014. Its publication has been delayed to allow the NCP's Steering Board to consider a request for a review of the NCP's procedure in handling the complaint. The request was subsequently found to be ineligible (see Annex 1).**

The complaint

1. The Non-Government Organisation (NGO), which campaigns on the international human right to privacy, complained about the impact of mass interception and surveillance of private communications.[1]

2. The NGO identified six telecommunication companies who are either UK based or are US multinationals with UK operations, it alleges to have collaborated with UK Government security services in facilitating access to undersea fibre optic cables that the companies own, operate or control.

3. The NGO argued that the human right to privacy is an internationally recognised right; mass interception and surveillance of private communications is a violation of the individual's human right to privacy; and that, therefore, by assisting UK Government entities, in responding to an interception warrant in a manner that goes beyond their legal obligations to that government, the companies have contributed to an infringement on the human right to privacy.

4. The NGO has brought this complaint to the UK National Contact Point (NCP) complaints process in order to resolve the issues raised. The NGO is also pursuing proceedings in the Investigatory Powers Tribunal (IPT) against the UK government services concerned.

Responses from the companies

5. Each of the companies identified by the complainant responded to the complaint. None of the responses disputed that the company responding owned, operated or controlled fibre optic cables or the associated shore-side facilities.

[1] *Telephone or the content of customer's private emails or correspondence*

6. Individual company responses were as follows:

Company 1

7. In its 16 December 2013 response to the complaint, Company 1 refuted the allegations presented. The company stated that the statutory duty placed on it under section 19 of the Regulation of Investigatory Powers Act 2000 (RIPA)[2] and section 5 of the Official Secrets Act prohibits it from disclosing any details relating to an interception request.

8. The company also stated that it had not knowingly contributed to human rights violations, and that it fully met its obligations both within the scope of the law and under the Guidelines. It questioned the basis of the NGO's complaint, in particular its interest in the matter.

9. The company did not accept that there was a positive legal obligation on it to challenge interception warrants citing section 11(4) of RIPA:

"it shall (subject to subsection (5)) be the duty of that person to take all such steps for giving effect to the warrant as are notified to him by or on behalf of the person to whom the warrant is addressed" and

section 11 (7): *A person who knowingly fails to comply with his duty under subsection (4) shall be guilty of an offence and liable - (a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both; (b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both"*.

10. The company stated that the complaint substantially covers the same grounds as the proceedings brought before the Investigatory Powers Tribunal (IPT)[3] to which it has, in its response to the NGO' solicitor, made clear that if required, it would fully cooperate.

Company 2

11. In its response of 17 December 2013, the company refuted the complaint and stated that the issue falls outside the scope of the NCP and OECD Guidelines, particularly in view of the statutory duty placed on it under RIPA.

12. The company went on to state that the IPT, to whom the NGO has already brought a challenge to the use of RIPA, is best placed to resolve the issue.

---

[2] *RIPA places a legal duty on telecommunication companies to assist Government entities in undertaking proportionate surveillance by way of an interception warrant for the purpose of preventing or detecting serious crime, and safeguarding the economic well-being of the UK by way of an Interception warrant which is issued in respect of one person as the interception subject or single set of premises to which an interception is to take place, thereby limiting interception to a specified range of targets.*

[3] *the body responsible for dealing with complaints of improperly used data or surveillance by public bodies*

13. The company stated that it is fully supportive of the principles of the Guidelines' General Policies and in this regard, its customers' privacy is of paramount importance.

14. In demonstrating its compliance with the law in all the countries in which it operates, the company cites the following international policies that as an organisation it is compliant with, including:

EU Privacy Directive[4];
EU Data Retention Directive[5];
European Convention on Human Rights[6]

Company 3

15. In its response of 18 December 2013, the company refuted the complaint and any suggestion that it provided unauthorised access to its network to any Government and confirmed that, only where mandated by the law, does it provide UK Government entities with access to customer data.

16. The company stated that it is both its practice and policy to review each request to ensure that the agency has the authority to compel it to provide access to such data. The company carefully monitors access to ensure that the data disclosed is only the data that must be disclosed under the law.

17. It is only in exigent circumstances involving imminent and substantial harm to life or property that its policies provide for some flexibility in allowing law enforcement bodies access to limited data in advance of receipt of a warrant or court order. Law enforcement bodies are required to provide authorisation paperwork for each exigent request.

18. The company states that the complaint by the NGO that "any mass Government surveillance programme is a violation of international law and the European Convention on Human Rights because it can never be necessary and proportionate" runs contrary to existing UK legislation on lawful interception of data as set out in the Code of Practice issued by the Secretary of State in relation to RIPA that makes clear that any lawful interception of data must be a "justifiable interference with an individual's right under Article 8 of the European Convention on Human Rights[7].

---

[4] *provides a fundamental right that personal data can be collected and stored only under strict conditions and for limited purposes and places a duty on managers and keepers of personal data to protect it from misuse and respect the individuals rights)*

[5] *requires telecommunication operators to retain certain categories of data (for identifying users and details of phone calls made and emails sent, excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism)*

[6] *"Everyone has the right to respect for his private and family life, his home and his correspondence; there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others")* .

[7] *The right to privacy*

Company 4

19. In its response of 6 January 2014, the company made it clear that it was prohibited from responding to the specific complaints made by the NGO, as in doing so it would give rise to a criminal offence in contrary to Section 19 of RIPA.

20. The company stated that its customers' data privacy is paramount to it and its policies ensure that data protection rights are safeguarded in a manner that provides protection of the underlying privacy rights and requires every request for access to data to be:

- authorised by security and legal senior managers;
- analysed in respect of its viability from a technical perspective; and
- analysed and reviewed to ensure it meets the applicable legislative requirements

21. The company stated that:
- It felt premature to seek to determine a matter within the OECD complaints process when the challenge on the lawfulness and proportionality of interception warrants, brought before the IPT by the NGO, is still being reviewed.
- It does not have publicly available policies, as it provides business solutions to customers who procure ICT solutions through tenders or direct contact and does not serve individual consumers. This means that a public declaration of its position on these matters has not been necessary, but is however available to customers on request.
- To demonstrate its effective governance and protection of data security, its sales process often includes due diligence activities that require evidence of policies, processes and procedures

22. The company concluded that its strict data protection standards offer high levels of propriety and this, together with confidentiality for customer data and services, pays due regard to its human rights obligations.

Company 5

23. In its response dated 10th January the company stated that the legal framework, in particular under Section 19 (1) [1] of RIPA and Section 94(5) of the Telecommunications Act 1984[2] would prohibit voluntary disclosure of anything done by virtue of any order, if any such order had been served.

24. The company outlined:
(I) the restrictions that impede it from responding to the specific allegation of collaborating with the Government;
(II) an overview of how it responds to the human right to privacy and freedom of expression obligations under the OECD Guidelines;

(III) the powers under which the target of surveillance need not be specified;
(IV) the provisions under which it exceptionally provides voluntary assistance in the interception of data; and
(V) its current policies which ensure the human right to privacy is respected.

25. The company stated that the proceedings already launched with the IPT by the NGO seemed to be the appropriate approach to consider the issues raised.

Company 6

26. In its response of 31 January, the company stated that it considered that the allegations presented were false and without foundation in their entirety, and that the NCP was not the appropriate forum for any investigation.

27. The company stated that it would never:
(I) Knowingly permit any form of access to customer data, beyond that which is mandated by law, for example disclosures under RIPA.
(II) Accept any instruction for access to data beyond its jurisdiction, or exceed its legal obligation by deliberately collaborating in order to open up its networks to any form of mass observation by the Government of any country.

28. The company stated that the appropriate jurisdiction for any investigation relating to these allegations rests with the IPT and not the NCP.

29. The company also stated that it complies with the law in all of the countries it operates in, including in respect of the: EU Privacy Directive; EU Data Retention Directive, and European Convention on Human Rights.

30. In conclusion the company maintained that it takes the matter of privacy for its customers and legal obligations in respect of data protection and data retention extremely seriously.

Guidelines provisions cited

31. The provisions cited by the NGO are listed below after this paragraph. The NGO has cited provisions under both the 2000 and 2011 versions of the Guidelines as it is unclear as to when the alleged actions actually took place. Most of the 2011 provisions cited were newly added to the Guidelines in 2011 and are applied by the UK NCP to activities of enterprises from 1 September 2011 and to ongoing impacts known to enterprises at that date. The NCP notes that some of the provisions identified are expressed as actions enterprises are encouraged rather than obliged to take:

2011 Guidelines

Chapter II General Policies

Enterprises should take fully into account established policies in the countries in which they operate, and consider the views of other stakeholders. In this regard:

A) Enterprises should:

2. Respect the internationally recognised human rights of those affected by their activities.[8]

10. Carry out risk-based due diligence, for example by incorporating it into their enterprise risk management systems, to identify, prevent and mitigate actual and potential adverse impacts as described in paragraphs 11 and 12, and account for how these impacts are addressed. The nature and extent of due diligence depends on the circumstances of a particular situation.
11. Avoid causing or contributing to adverse impacts on matters covered by the *Guidelines*, through their own activities, and address such impacts when they occur.

12. Seek to prevent or mitigate an adverse impact where they have not contributed to that impact, when the impact is nevertheless directly linked to their operations, products or services by a business relationship. This is not intended to shift responsibility from the entity causing an adverse impact to the enterprise with which it has a business relationship

B) Enterprises are encouraged to:

1. Support, as appropriate to their circumstances, cooperative efforts in the appropriate fora to promote Internet Freedom through respect of freedom of expression, assembly and association online.

Chapter IV Human Rights

States have the duty to protect human rights. Enterprises should, within the framework of internationally recognised human rights, the international human rights obligations of the countries in which they operate as well as relevant domestic laws and regulations:

1. Respect human rights which means they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

[8] This provision also appears, and is cited by the complainants, in the 2000 Guidelines

2. Within the context of their own activities, avoid causing or contributing to adverse human rights impacts and address such impacts when they occur.
3. Seek ways to prevent or mitigate adverse human rights impacts that are directly linked to their business operations, products or services by a business relationship, even if they do not contribute to those impacts.
4. Have a policy commitment to respect human rights.
5. Carry out human rights due diligence as appropriate to their size, the nature and context of operations and the severity of the risks of adverse human rights impacts.

2000 Guidelines

Chapter III Disclosure

5. Enterprises are encouraged to communicate additional information that could include:

a. Value statements or statements of business conduct intended for public disclosure including information on the social, ethical and environmental policies of the enterprise and other codes of conduct to which the company subscribes. In addition, the date of adoption, the countries and entities to which such statements apply and its performance in relation to these statements may be communicated.

b.Information on systems for managing risks and complying with laws, and on statements or codes of business conduct.

The Initial Assessment process

32. The Initial Assessment process is simply to determine whether the issues in the complaint merit any further examination. **It does not determine whether a company has breached the Guidelines**.

Handling process

33. The UK NCP notes that there has been a significant delay in its handling of this complaint, and offers its apologies to the parties for this. A number of factors contributed to the delay including temporary resourcing and technical issues as well as the multiple parties involved.

34.

04.11.13	NCP receives NGO complaint
15.11.13	NCP shares complaint with company and invites response.
16.12.13	NCP receives Company 1' response
17.12.13	NCP receives Company 2' response
18.12.13	NCP receives Company 3' response

06.01.14	NCP receives Company 4' response
10.01.14	NCP receives Company 5' response
31.01.14	NCP receives Company 6' response
15.04.14	NCP shares response with parties
16.04.14	NCP receives comments from Company 1
17.04.14	NCP receives comments from Company 2
01.05.14	NCP receives comments from Company 5
01.05.14	NCP receives comments from complainants

35. All the documents submitted have been shared with the NGO and the respective companies. As part of the NCP process for dealing with complaints brought under the OECD Guidelines, each party was offered an initial meeting to explain the complaints process;. Company 2 was the only party that requested a meeting with the NCP to discuss the handling process. This meeting took place on 18th December 2013.

UK NCP decision

- **The UK NCP has decided to reject the complaint on the basis that the NGO has not been able to substantiate the allegations. The UK NCP took the following points into account when considering whether the complainant's concerns merited further examination:**

Identity of the complainant and their interest in the matter:

36. The NGO has an established reputation for campaigning for the universal human right to privacy. The NCP is satisfied that it has a valid interest in the issues raised.

37. The NCP notes that the NGO does not identify specific individuals or groups that it represents; the NCP understands that those affected potentially include every person whose communications into or out of the UK and Europe where routed through the fibre optic cables to which the NGO's complaint refers.

Whether the issue is material and substantiated:

38. The NGO claims that fibre optic cables that carry the majority of the world's network traffic[9] are capable of landing in multiple countries and facilitating access to these cables provides the UK Government, given the country's unique position on the edge of Europe, with disproportionate access to cables emerging from the Atlantic.

39. The NGO also highlights concerns over a perceived risk of intercepted data ending up in the hands of other states as a result of a secret alliance of five countries[10].

[9] *Communications ranging from phone calls to emails to any form of information conveyed over the internet*
[10] *Five Eyes Alliance (US, the UK, Australia, Canada and New Zealand) alleged to have been sharing data*

40. To support its case, the NGO provides documents to support its argument that:

(I) The human right to privacy is an internationally recognised right.[11]

(II) Mass interception and surveillance of private communications that rely on the collection and storage of data related to an individual's private life, infringes on an individual's human right to privacy[12].

(III) Surveillance and interception of communication, wire-tapping and recording of conversations should be prohibited[13].

(IV) Placing taps on the fibre optic cables, and applying word, voice and speech recognition, allows states to achieve almost complete control of tele and online communications, and this kind of mass intercept technology eradicates any considerations of proportionality, thereby enabling indiscriminate surveillance[14]

(V) The right to privacy is essential for individuals' rights to freedom of expression. Monitoring and collecting information about an individual's communications and activities on the internet, "can constitute a violation of the Internet user's right to privacy, and by restricting people's anonymity and confidence on the Internet, it impedes the free flow of information and ideas online."[15]

(VI) The existence of legislation which allows secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied[16]. This threat strikes at freedom of communication between users of the telecoms services, thereby amounting to an interference with the exercise of the user's rights under Article 8.[17]

41. The NGO states that the media have implicated the companies as having enabled access by UK Government agencies to fibre optic cables or the shore-side facilities associated with the cables and then sharing the information it collects with the US National Security Agency (NSA).

42. The NGO asserts that by facilitating access to its infrastructure, the companies have enabled mass interception and indiscriminate collection of data and in doing so knowingly contributed to human rights violations and questions whether the companies contravened the OECD Guidelines for Multinational Enterprises.

NCP Findings

[11] *Article 17 (1) of the International Covenant on Civil and Political Rights*
[12] *Article 8 of the European Convention on Human Rights*
[13] *No 16 of the UNHRC' General Comments*
[14] *No 16 of the UNHRC' General Comment*
[15] *The UN Special Rapporteur*
[16] *The European Court of Human Rights*
[17] *Weber and Saravia v Germany*

43. In support of its claims, the NGO provides a range of press reports containing allegations relating to the UK Government's interception activities, as well as EU reports on issues relating to infringements of the human right to privacy and freedom of expression on the Internet. The NCP notes that the claims made in many of the press reports are based on unofficially obtained UK Government documents that are no longer accessible.

44. The UK NCP understands that it is generally acknowledged by the UK Government that it carried out interceptions, although it is not accepted that these actions broke relevant laws and standards. The UK NCP accepts that the information provided shows that the privacy issues raised are relevant to the human rights related obligations of enterprises under the Guidelines. The link the complainants make to the specific companies identified in the complaint does not appear to the UK NCP to be substantiated, however. It depends on a single press report about the contents of a document alleged to have been produced by UK security services.

45. The UK NCP accepts that the publication that made this report saw the document concerned and had reason to trust the source providing it, who had provided other information generally acknowledged to be genuine. The document (which appears to date from 2009) is not available to any party in the complaint, however, and the NCP also notes that None of the companies identified in the document appears to have been aa party to it (i.e. it is reported to be an internal document and not a contract or other type of agreement). The NCP does not consider that this information substantiates a link between the activities of the enterprises identified and the issue raised.

46. The NCP notes that the companies do not explicitly deny receiving the warrants in question. From the information provided, it appears that this is because of legitimate concerns that commenting on whether and what warrants may have been received would place the companies in breach of duties placed on them by RIPA. The NCP does not consider that the absence of an explicit denial substantiates an issue for further examination with regard to the specific allegations made. The NCP also notes that Chapter I Paragraph 2 of the OECD Guidelines clearly states that obeying domestic laws is the first obligation of enterprises and that the Guidelines "*should not and are not intended to place an enterprise in situations where it faces conflicting requirements"*.

47. The NCP finds that the NGO presents a strong case that mass interception and surveillance of private communications through the collection and storage of data relating to an individual's private life can infringe an individual's human right to privacy.

48. The NCP also recognises that any activity by a company that causes, facilitates or incentivises human right impacts would place a duty on the company, under the OECD guidelines, to apply due diligence.

49. However, the NCP considers that the information provided in the complaint and response does not substantiate a link between the companies named in the complaint and the activities described in the complaint.

50. Given that none of the companies disputed that they owned, operated, or controlled fibre optic cables, the NCP considered whether information provided about the UK Government's access to these cables indicated that there was a general issueabout the adequacy of the companies' due diligence procedures, regardless of whether or not the companies co-operated in providing this access.

51. The NCP concluded, however, that the issue of due diligence was raised with regard to the specific allegations in the complaint, which have not been substantiated. The NCP process is not intended to initiate a wider examination of the sector in question, in this case, the due diligence of all companies operating in this sector in relation to interception requests. This would be outside the scope of the NCP process as envisaged in the Guidelines. It would therefore be unfair for the NCP itself to raise a wider due diligence issue that the complainant had not intended and to which the companies had not been given a fair opportunity to respond.

Relevance of applicable law and procedures, including court rulings

52. The issues highlighted by the NGO relate to:

(I) The international law on human rights under the International Convention on Civil and Political Rights which provides that *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation*;

(II) Article 8 of the European Convention on Human Rights, which provides both that:

- *all individuals have the human right to respect of their private and family life, their home and their correspondence;*
- *no public authority should interfere with the exercise of that human right except in:*

a) *accordance with the law*
b) *where it is necessary in the interests of national security, public safety or the economic wellbeing of the country,*
c) *for the prevention or disorder of crime,*

d) *for the protection of health or morals, or*
e) *for the protection of the rights and freedoms of others and*
f) *where necessary in accordance with the above mentioned, is proportionate.*

53. Under UK domestic law, UK Government entities are responsible for justifying that any infringement on the human rights provided under Article 8 is proportionate in pursuit of a legitimate aim.

54. The duty to comply with the law is placed on the Government entity (acting in order to prevent or detect serious crime and to safeguard the economic well-being of the UK) and the company in question (which must comply with RIPA).

How similar issues have been, or are being, treated in other domestic of international proceedings:

55. The UK NCP notes similarities between this case and other recent NCP cases relating to the supply of ICT services and links to human rights abuses: including a complaint from the NGO Reprieve against British Telecommunications plc (BT) and a complaint from the NGO Privacy International against Gamma International. Initial Assessments setting out the issues in these cases appear on the UK NCP webpage.

56. In each case, the NCP has considered the information provided in the complaint and the response from the company to determine whether there is a substantiated link between the company and the alleged abuse described in the complaint.

Whether the consideration of the specific issue would contribute to the purpose and effectiveness of the Guidelines

57. The NCP's decision is principally based on its findings about whether the issues raised are material and substantiated, rather than on an assessment of the likely outcome of further examination.

58. The NCP notes however that the NGO has already brought a challenge around the use of RIPA to the IPT which exists to investigate complaints about the alleged conduct including improper use of data/surveillance by UK Government entities within the scope of RIPA.

Next steps

59. As the complaint has been rejected, this Initial Assessment concludes the complaint process under the Guidelines.

Date: 11 July 2014
UK National Contact Point for the OECD Guidelines for Multinational Enterprises

Steven Murdoch
Danish Chopra
Liz Napier
Sammy Harvey

Annex 1: Request for review of the NCP's procedure in this complaint

1. At the conclusion of the UK NCP complaint procedure, a party can request a review if it considers that the NCP did not follow proper or fair procedure in considering a complaint.

2. Full details of the UK NCP review procedure can be found at: https://www.gov.uk/government/publications/complaints-brought-under-the-oecd-guidelines-for-multinational-enterprises-to-the-uk-national-contact-point-review-procedure . Reviews are conducted by the NCP's Steering Board and consider procedure: they do not address the substance of complaints or NCP decisions. An assessment subject to a review request is not generally published until the review is completed.

3. In this complaint, the complainant informed the NCP on 24th July of its request for review, and subsequently provided particulars setting out a case that the UK NCP had incorrectly applied initial assessment criteria included in its procedures (as revised at January 2014) and relating to whether the issues in the complaint are material and substantiated and whether there seems to be a link between the enterprise's activities and the issues raised.

4. Paragraph 4.3 of the review procedure states that the NCP can recommend at any time that the Board dismisses a review request as ineligible, frivolous or vexatious. A recommendation of this kind by the NCP stands unless three or more Steering Board Members object.

5. The NCP recommended to the Steering Board on 2nd September 2014 that the Board refuse the complainants' request as ineligible because no error of procedure was identified. The Steering Board discussed this recommendation at its meeting on 17th September 2014. Only one objection was subsequently received and on 6th October the NCP informed parties that the review request was refused and the Initial Assessment issued on 11th July 2014 would now be published.