

---

# REPRIEVE

---

## Complaint to the UK National Contact Point under the Specific Instance Procedure of the OECD Guidelines for Multinational Enterprises: BT Group plc

19 August 2014

### Contents

1. Summary of complaint
2. Introduction
3. Procedural Background
4. New Evidence of BT's Role in US Drone Programme and Mass Surveillance
5. Breaches of the OECD Guidelines
6. Conclusion
7. Supporting documentation

#### 1. Summary of complaint

1.1. Reprieve submits that BT Group plc (BT) has breached the OECD Guidelines by:

- (i) Contracting with the US government's Defense Information Systems Agency (DISA) to supply a fibre-optic communications cable that connects RAF Croughton to Camp Lemonnier. RAF Croughton provides "global strike operations"<sup>1</sup> and Camp Lemonnier is the "most important base for drone operations outside the war zone of Afghanistan".<sup>2</sup> Consequently, BT's cable likely supports the round-the-clock drone strikes in Yemen and Somalia operated by the United States Air Force and Central Intelligence Agency as part of its "targeted killing" programme. Without a declared war, these drone strikes are used in an opaque and secretive manner without any supervision or accountability, a clear violation of international law.

---

<sup>1</sup> "RAF Croughton: 422<sup>nd</sup> Air Base Group", <http://www.501csw.usafe.af.mil/units/croughton>.

<sup>2</sup> "Death From Afar", *The Economist* (3 November 2012) <http://www.economist.com/news/international/21565614-america-uses-drones-lot-secret-and-largely-unencumbered-declared-rules-worries>.

- (ii) Facilitating the blanket surveillance of telecommunications by the Government Communications Headquarters (GCHQ), the National Security Agency (NSA), and other intelligence agencies. This mass data collection has been openly acknowledged as a key part of drone targeting.<sup>3</sup>
- (iii) Failing to provide evidence of due diligence mechanisms showing how the company has sought to prevent, address, or mitigate the human rights impacts to which it appears to be contributing, as required in order to comply with the OECD Guidelines. Based on the foreseeable use of the cable for US military drone strikes and on the risk that mass surveillance data may be used in drone targeting, BT has the responsibility to “demonstrate that they have complied with the due diligence requirements of the Guidelines and taken ‘necessary steps to cease or prevent its contribution’ to any risk of harm.”<sup>4</sup>

## 2. Introduction

- 2.1. Reprieve is a legal action charity working to safeguard the human rights of people impacted by counter-terrorism operations conducted by the US and other governments. Reprieve’s work includes investigation and advocacy in relation to the use of US drones in non-war zones.
- 2.2. Reprieve is bringing this complaint on behalf of its clients in Yemen (*e.g.*, Mohammed al-Qawli,<sup>5</sup> Faisal bin Ali bin Jaber<sup>6</sup>) whose fundamental human rights have been grossly violated by the extensive US drone attacks.
- 2.3. BT Group plc (BT) is a major provider of global telecommunications networks and services in more than 170 countries. The company is headquartered at 81 Newgate Street, London EC1A 7AJ.
- 2.4. Reprieve first presented the issue of BT’s potential complicity with US drone strikes to the UK National Contact Point (UK NCP) in an OECD complaint dated 15 July 2013. Unfortunately, the UK NCP declined to advance the complaint beyond the Initial Assessment stage, on the basis that Reprieve had not provided a “specific link” between BT and the US drone programme.<sup>7</sup>

---

<sup>3</sup> Lee Ferran, “Ex-NSA Chief: ‘We Kill People Based on Metadata’”, ABC News (12 May 2014) <http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata>.

<sup>4</sup> UK NCP Review Committee, “Application for Review of the Initial Assessment – Recommendation of the Review Committee”, pp. 5-6 (17 January 2014)

<sup>5</sup> Mohammed al-Qawli, “The US killed by brother with a drone. I want to know why.” *Al Jazeera* (5 December 2013) <http://america.aljazeera.com/opinions/2013/12/grieving-yemena-sinnocentdead.html>.

<sup>6</sup> Daniel A. Medina, “Yemeni man seeks answers in US over deadly drone strike.” *Al Jazeera* (19 November 2013) <http://america.aljazeera.com/articles/2013/11/19/yemeni-activist-seeksanswersondronestrikethatkilledrelatives.html>.

<sup>7</sup> With citation to Reprieve’s earlier OECD complaint against BT, OECD Watch has documented the “troubling trend” of “NCPs increasingly expecting complainants to satisfy an unreasonably high burden of proof before even accepting a complaint and seeking to bring the parties together for dialogue”. *Assessment of NCP Performance in the 2013-2014 Implementation Cycle*, p. 18, OECD Watch (14 June 2014) [http://oecdwatch.org/publications-en/Publication\\_4090/at\\_download/fullfile](http://oecdwatch.org/publications-en/Publication_4090/at_download/fullfile).

- 2.5. As a result, BT’s strategy of willful ignorance was given the stamp of approval by the UK NCP, sending the uncomfortable message that companies can avoid responsibility by simply refusing to investigate human rights abuses. Despite the company’s complete failure to disclose any information regarding its due diligence efforts, the rejection of Reprieve’s complaint by the UK NCP has been used persistently by BT as a decisive ruling absolving them of all potential wrongdoing and further obligations. As such, the UK NCP’s failure to properly investigate Reprieve’s prior complaint has not only allowed BT to continue to operate unchecked, it has permitted BT to positively assert a clean human rights record.
- 2.6. After the UK NCP rejected Reprieve’s complaint, journalists began investigating BT’s activities. Fresh evidence was uncovered suggesting BT had constructed the fiber-optic cable with full knowledge that the communications line would utilise Defense Information Systems Network (DISN) routers and KG-340 encryption devices. These elements of the fibre-optic cable were installed to fit specific NSA requirements to ensure the security necessary to process intelligence data and to issue commands for drones.
- 2.7. Reprieve brought the new evidence to the UK NCP’s attention on 29 May 2014, but the Treasury Solicitor’s Department indicated that a fresh complaint to the UK NCP should be made.
- 2.8. Thus, pursuant to section 3.6.4 of the UK NCP procedures<sup>8</sup> and in light of the newly uncovered information about the Croughton-Lemonnier cable and mass surveillance, Reprieve is submitting this new complaint in hopes that the UK NCP will call on BT to be transparent about its knowledge and involvement in the US drone programme.

### 3. Procedural Background

26 September 2012	BT signs the STM-16 fibre-cable contract with US government.
17 January 2013	Reprieve sends inquiry letter to BT about the contract.
24 January 2013	BT responds with a letter to Reprieve declining to comment.
15 July 2013	Reprieve files a complaint against BT with UK NCP.
24 July 2013	UK NCP shares complaint with BT and invites a response.
20 August 2013	BT files a response with UK NCP.
October 2013	UK NCP shares draft Initial Assessment with Reprieve and BT.

<sup>8</sup> “A complainant may submit a new complaint in respect of issues rejected by the NCP if new information means the reasons for rejection no longer apply”.

24 October 2013	Reprievе sends a letter to UK NCP to request a review of Initial Assessment by the Steering Board.
12 November 2013	UK NCP sends a letter to notify Reprievе that the request had been sent to the Steering Board to establish a Review Committee and that any further comments could be submitted until 19 November 2013.
19 November 2013	Reprievе sends a letter to UK NCP with additional submissions on the application for review.
17 January 2014	The Review Committee releases its recommendation to decline further review by the Steering Board.  The Review Committee also issues a separate policy note on due diligence.
19 February 2014	UK NCP publishes the final version of the Initial Assessment.
1 May 2014	Reprievе sends a Letter Before Claim, seeking judicial review of the UK NCP’s failure to properly address the complaint.
15 May 2014	Treasury Solicitor’s Department replies to Reprievе, rejecting any claims made regarding the unlawful and unfair nature of the UK NCP’s decision.
29 May 2014	Reprievе writes to Treasury Solicitor’s Department, presenting fresh evidence of BT complicity in drone warfare and encouraging UK NCP to reopen the investigation.
13 June 2014	Treasury Solicitor’s Department replies to Reprievе, refusing to consider the fresh evidence.

- 3.1. Reprievе wrote a letter on 17 January 2013 to BT, seeking clarification of the company’s involvement with US counter-terrorism operations at Camp Lemonnier: background of the contract, BT’s precise obligations, status of implementation, BT’s policy with regards to supporting the use of weaponised drones, and any due diligence/risk assessment policies with regards to potential violations of international law.
- 3.2. BT Legal responded on 24 January 2013 with a letter indicating that BT would not disclose contractual matters and that Reprievе should address any further queries to the US government.

- 3.3. On 15 July 2013, Reprieve filed an OECD complaint against BT with the UK NCP.
- 3.4. On 20 August 2013, BT filed a response to Reprieve's complaint, denying any breach of the OECD guidelines. BT argued the following:
  - (1) Reprieve did not qualify as an 'interested party' for filing the complaint,
  - (2) the legality of the drone strikes was still being debated,
  - (3) only speculative evidence linked usage of the STM-16 with American drone activity,
  - (4) the STM-16 is a general purpose system that BT did not design for military purposes, and
  - (5) BT had no way of monitoring the content passed through the STM-16.
- 3.5. In October 2013, the UK NCP shared a draft Initial Assessment with BT and Reprieve that indicated the issues raised by Reprieve did not merit further examination.
- 3.6. On 24 October 2013, Reprieve sent a letter to UK NCP to request a review of the draft Initial Assessment by the Steering Board. Reprieve asserted procedural defects in that
  - (1) the UK NCP had overly relied on BT's assertions (*i.e.*, press statements) in lieu of the significant amount of public domain information regarding drone strike activities at Camp Lemonnier, and
  - (2) the UK NCP had taken no steps to draw out information from BT regarding the nature and uses of the services provided to the United States government.
- 3.7. On 12 November 2013, the UK NCP notified Reprieve that it had forwarded the request to its Steering Board to establish a Review Committee and that any further comments could be submitted until 19 November 2013. The UK NCP noted that the Initial Assessment stage of a complaint was a 'desk-based analysis' that considers the information submitted to it, and that it considered Reprieve as the complainants to have full responsibility to connect BT to the drone attacks.
- 3.8. On 19 November 2013, Reprieve provided the UK NCP with clarifications to the application for review, noting that while independent research into BT's representations was not required, the UK NCP had not conducted even a minimal level of research. Reprieve also asserted that even if the onus were on Reprieve to substantiate a link between BT and the drone attacks, BT had refused to cooperate in any way, making it effectively impossible to uncover the necessary information.
- 3.9. On 17 January 2014, the UK NCP Review Committee released its recommendation to the Steering Board to decline further review, finding no procedural defects because it is not the role of a NCP to conduct research at the Initial Assessment phase. The Review Committee emphasized also that its own role was limited to analysing the procedural elements of the NCP's decision, meaning the substantive decision of insufficient

evidence could not be altered. However, the Review Committee did recognize the need to clarify in a separate note to the Steering Board regarding what is required to trigger a company's due diligence obligations under the OECD Guidelines.

- 3.10. Reprieve respectfully requests that the UK NCP formalise the Review Committee's due diligence notes into formal guidelines in order to clarify the issue for businesses, civil society, and other stakeholders.
- 3.11. On 17 January 2014, the Review Committee also issued a separate policy note on due diligence. The note stated that foreseeability should be the factor to bear in mind for interpreting the due diligence requirements. In addition, if the goods or services of a company carry an inherent risk of harm or if the activities or reputation of the customer give rise to such a risk, the principle of due diligence requires a company to conduct the necessary inquiries before delivering anything. Specifically, the Review Committee indicated that it is the company's responsibility to demonstrate compliance with due diligence requirements and to take the required steps to cease or prevent contribution to any risk of harm. A failure by the company to do so would substantiate an OECD Guidelines complaint.
- 3.12. On 1 May 2014, Reprieve sent a Letter Before Claim seeking judicial review of the UK NCP's failure, *inter alia*, to uphold the OECD Guidelines in ignoring the following relevant considerations:
  - (1) The Guidelines do not require Reprieve to show a specific link between BT's contract with the US military and adverse human rights consequences.
  - (2) The activities and reputation of the US military triggered BT's obligation to conduct at least general due diligence inquiries into the human rights consequences of its services and products.
  - (3) In line with the Review Committee's separate policy note, BT was under a stricter due diligence obligation because it was foreseeable that the fibre-optic cable would be used in the US drone programme.
- 3.13. The Treasury Solicitor's Department responded on 15 May 2014, arguing that the UK NCP was not subject to judicial review as an entity that exists only to fulfill UK's international treaty obligations. It also repeated the UK NCP's contention that the body has no duty to inquire or investigate a complaint.
- 3.14. At the beginning of May, fresh evidence came to light which further strengthened Reprieve's claims that BT had knowingly constructed the cable for the US military to use in its drone operations, as well as more details on how BT is a key partner in the mass surveillance conducted by various intelligence agencies.
- 3.15. On 29 May 2014, Reprieve compiled a letter to the Treasury Solicitor containing the evidence of BT's complicity that had emerged in the time period that followed the

original OECD complaint.

- 3.16. Instead of the UK NCP reopening the investigation as requested, the Treasury Solicitor's Department indicated that Reprieve should simply file a new complaint against BT with the UK NCP.

#### 4. **New Evidence of BT's Role in US Drone Programme and Mass Surveillance**

- 4.1. For a detailed overview of the US drone programme and the onerous impact on human rights, please see Section 4 ("Overview of Targeted Killing Programme") of the prior OECD complaint by Reprieve filed on 15 July 2013.<sup>9</sup>

##### *BT Continues to Ignore Evidence of its Complicity with US Drone Programme*

- 4.2. BT's approach to human rights focuses on maintaining an implausible ignorance of relevant facts: the company refuses to conduct internal investigations, dismisses journalists as speculative, and ignores evidence as non-factual.
- 4.3. BT has repeatedly insisted that (1) the fibre-optic cable connecting the two bases is a general purpose one and that (2) the company has no knowledge or involvement in military applications of the cable.
- 4.4. For example, in its latest "Better Future" report released May 2014, BT includes the following:

*BT can categorically state that the communications system mentioned in Reprieve's complaint is a general purpose fiber-optic system. It has not been specifically designed or adapted by BT for military purposes. BT has no knowledge of the reported US drone strikes and has no involvement in any such activity. BT takes its human rights obligations very seriously and is fully supportive of the OECD Guidelines.*<sup>10</sup>

- 4.5. Despite all the information in the public domain that the cable enables the US drone strikes from Camp Lemonnier, BT wants the general public to believe that it has never heard of the issue. BT has been well-informed of the significant risk it is complicit in the drone programme and it should bear the responsibility of responding appropriately.
- 4.6. The most recent instance of BT's policy of willful ignorance was articulated at its annual general meeting (AGM) on 16 July 2014. At the AGM, Reprieve asked BT's board of directors whether the company's board-level review of its overarching human rights policy or its compliance framework for human rights would encompass BT's role

---

<sup>9</sup> Reprieve, "Complaint to the UK National Contact Point under the Specific Instance Procedure of the OECD Guidelines for Multinational Enterprises in respect of BT plc" (15 July 2013)

[http://www.reprieve.org.uk/media/downloads/2013\\_07\\_15\\_PUB\\_Complaint\\_to\\_UK\\_NCP\\_re\\_BT\\_plc.pdf](http://www.reprieve.org.uk/media/downloads/2013_07_15_PUB_Complaint_to_UK_NCP_re_BT_plc.pdf).

<sup>10</sup> BT Group, "Better Future Report 2014" (May 2014)

[http://www.btplc.com/betterfuture/betterfuturereport/pdf/2014/Better\\_Future\\_report2014-complete\\_report.pdf](http://www.btplc.com/betterfuture/betterfuturereport/pdf/2014/Better_Future_report2014-complete_report.pdf).

in the US drone programme.<sup>11</sup>

4.7. Sir Michael Rake, Chairman of BT's board of directors responded:

*We are not a military provider, of military equipment. We have no knowledge of the use or what's being done; we have no possible basis for challenging people on how they use our telecommunications equipment, providing they pay for it, and providing they're not subject to legal sanction.*

#### *BT Knowingly Modified the Croughton-Lemonnier Fibre-Optic Cable for Military Purposes*

4.8. However, investigations by *Computer Weekly* revealed on 2 May 2014 how BT's contract with the US government for the Croughton-Lemonnier connection stipulated that the cable would be a part of the Defense Information Systems Network (DISN) – the core of the Global Information Grid (GIG), a military internet spanning 3500 US facilities in at least eighty-eight countries.<sup>12</sup>

4.9. While the DISN does carry a variety of military data traffic, the large bandwidth required for drone operations relies heavily on this network.<sup>13</sup> The US Department of Defense 2013-2036 Unmanned Systems Roadmap specified last December that drones rely on DISN connections for global distribution of mission data and for long-range command & control functions.<sup>14</sup>

4.10. Additionally, the contract specifies that DISN connection would operate at the highest security levels. To achieve this, BT capped its fibre-optic cable with KG-340 encryption devices built specifically to National Security Agency Type-1 Top Secret classification requirements and algorithms. The company undoubtedly knows or should know the KG-340 encryption devices are classified as High Assurance Internet Protocol Encryptors (HAiPE), key parts in constructing the GIG.<sup>15</sup>

4.11. The Croughton-Lemonnier line is therefore quite clearly not a general telecommunications line, contrary to what BT previously claimed and continues to claim. Day-to-day telecommunications at Camp Lemonnier have been provided by a local Djiboutian phone company, Djibouti Teleco since 4 February 2011.<sup>16</sup>

---

<sup>11</sup> See Zoe Williams, "The new breed of shareholder activist: taking on the big boys at the AGM", *The Guardian* (1 August 2014) <http://www.theguardian.com/business/2014/aug/01/new-breed-shareholder-activists>.

<sup>12</sup> Mark Ballard, "UK Telecoms Infrastructure Used to Support Controversial US Drone Operations", *Computer Weekly* (2 May 2014) <http://www.computerweekly.com/news/2240219969/UK-telecoms-infrastructure-used-to-support-controversial-US-drone-operations>.

<sup>13</sup> See Mark Ballard, "Drone kill communications net illustrated", *Computer Weekly* (13 June 2014) [http://www.computerweekly.com/cgi-bin/mt-search.cgi?blog\\_id=102&tag=HAiPE&limit=20](http://www.computerweekly.com/cgi-bin/mt-search.cgi?blog_id=102&tag=HAiPE&limit=20).

<sup>14</sup> Department of Defense, "Unmanned Systems Integrated Roadmap FY2013-2038" (23 December 2013) <http://www.defense.gov/pubs/DOD-USRM-2013.pdf>.

<sup>15</sup> *Id.*

<sup>16</sup> Kristine M. Sturkie, "NEXCOM Provides Internet Service to Military Members at Camp Lemonnier", *America's Navy* (8 February 2011) [http://www.navy.mil/submit/display.asp?story\\_id=58448](http://www.navy.mil/submit/display.asp?story_id=58448).



Consequently the line provided by BT is highly unlikely to serve a general telecommunications purpose. It is much more likely that the line supplied by BT is a bespoke product for the US military and intelligence agencies.

- 4.12. Despite these indications of military modifications, BT continues to dodge the question about the cable being used for drones, casually musing to journalists that the cable “could be used at the base for a wide range of day-to-day activities, such as general housekeeping/internet browsing, email, communications, stores ordering, data functions and voice communications.”<sup>17</sup>
- 4.13. The new evidence suggests BT installed the line with full knowledge it would upgrade the camps’ communications to allow the transmission of classified communications at the level required to form the “core communications backbone used by drone operations.”<sup>18</sup> Without BT’s careful construction of the line tailored to NSA requirements, RAF Croughton would not have the secure link necessary to process intelligence data and issue commands for the daily drone operations that fly out of Camp Lemonnier.

#### *BT Facilitates Covert Mass Surveillance and Drone Targeting by the UK and US Governments*

- 4.14. Fresh details have also emerged regarding BT’s involvement in the covert mass surveillance that has been acknowledged as a key part of how targeted people are chosen and subsequently murdered by drone.
- 4.15. In August 2013, *Süddeutsche Zeitung* and *The Guardian* revealed that along with six other telecommunications companies, BT had been secretly working with GCHQ and giving the agency access to its customers’ private communications without their knowledge or consent.<sup>19</sup>
- 4.16. On 3 June 2014, *The Register* provided additional details about how BT “operate[s] extensive long distance optical fibre communications networks throughout the UK, installed and paid for by GCHQ, NSA, or [...] NTAC”. BT and Vodafone were cited as the “two top earners of secret GCHQ payments running into tens of millions of pounds annually.”<sup>20</sup>

---

<sup>17</sup> Mark Ballard, “Telecoms Contractor Could be Called to Account for Drone Deaths”, *Computer Weekly* (21 March 2014) <http://www.computerweekly.com/blogs/public-sector/2014/03/telecoms-contractor-could-be-c.html>.

<sup>18</sup> Mark Ballard, “Analysis: How the UK Connects to the US Global Drone Network,” *Computer Weekly* (2 May 2014) <http://www.computerweekly.com/news/2240220017/Analysis-How-the-UK-connects-to-the-US-global-drone-network>.

<sup>19</sup> John Goetz & Frederik Obermaier, “Snowden enthüllt Namen der spähenden Telekomfirmen”, *Süddeutsche Zeitung* (2 August 2013) <http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791>; James Ball, Luke Harding, & Juliette Garside, “BT and Vodafone among telecoms companies passing details to GCHQ”, *The Guardian* (2 August 2013) <http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq>.

<sup>20</sup> Duncan Campbell, “Revealed: GCHQ’s Beyond Top Secret Middle Eastern Internet Spy Base”, *The Register* (3 June 2014) [http://www.theregister.co.uk/2014/06/03/revealed\\_beyond\\_top\\_secret\\_british\\_intelligence\\_middleeast\\_internet\\_spy\\_base](http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base).

- 4.17. Each time the intelligence agencies “wanted to tap a new international optical fibre cable, engineers from ‘REMEDY’ [BT’s codename] and would usually be called in to plan where the taps or ‘probe’ would physically be connected to incoming optical fibre cables, and to agree how much BT should be paid”.<sup>21</sup> This information strongly implicates BT in the provision of mass surveillance data necessary for the analysis and targeting of drone strikes.
- 4.18. Vast amounts of data from millions of internet users is stored for up to three days, while the metadata (*i.e.*, the sites visited by users, who emails whom, etc.) is kept for up to thirty days. The ex-head of the NSA, General Michael Hayden, has openly admitted that surveillance data and metadata is used to triangulate drone strikes in Yemen, Pakistan, and Somalia.<sup>22</sup> Information like the activity or location of a cell phone is used to make a simple guess at who may or may not be a militant, and a drone is sent to murder the individual.
- 4.19. At the BT AGM, Reprieve also asked the company’s board of directors whether BT planned to continuing assisting intelligence agencies in intercepting the data used to carry out drone strikes. BT’s response was again its standard position of ignorance and denial: “We cannot be held responsible, nor can we know, nor can we seek to know, the purpose for which people use our telecommunications equipment.”
- 4.20. When confronted with the extensive news stories on its complicity with mass surveillance and data retention, BT’s final word was broadly dismissive: “[T]he media stories and speculation isn’t necessarily anything we can use to change our position because it’s not factual.”
- 4.21. To date, BT has declined to even issue a transparency report, citing the issue at the recent AGM as a “political debate in which we don’t engage.” This lies in stark contrast to the position of other telecommunications companies such as Vodafone.<sup>23</sup>

## 5. Breaches of the OECD Guidelines

- 5.1. Enabled by the BT fibre-optics line and the company’s participation in mass surveillance, the US government’s “targeted killing” programme continues to violate the right to life and infringes numerous other internationally recognised human rights of those living in the affected areas:
- The right to freedom from torture, cruel, inhuman or degrading treatment (Universal Declaration of Human Rights (UNDH), Art 5);

---

<sup>21</sup> *Id.*

<sup>22</sup> *Supra* note 3.

<sup>23</sup> See Vodafone, *Law Enforcement Disclosure Report* (6 June 2014)

<http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires-allowing-state-surveillance>.

- The right to freedom from arbitrary or unlawful interference with privacy, family and home, as well as the right to the protection of the law against such interference or attacks (UNDH, Art 12);
- The right to freedom of peaceful assembly and association (UNDH, Art 20);
- The right to rest and leisure (UNDH, Art 24);
- The right to a standard of living adequate for the health and well-being of himself and of his family (UNDH, Art 25);
- The right to education (UNDH, Art 26);
- The right to freely participate in the cultural life of the community (UNDH, Art 27).

## Chapter II, General Policies

5.2. BT is in breach of the requirement in section A.2 to “[r]espect the internationally recognized human rights of those affected by their activities.”

5.3. Both by contracting to provide the fibre-optics backbone for the US drone programme and by facilitating mass surveillance by intelligence agencies, BT has demonstrated a complete failure to respect human rights.

## Chapter IV, Human Rights

5.4. Section 1 of Chapter IV states that enterprises should:

*“[r]espect 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.”*

5.5. Section 2 indicates that enterprises should:

*“[w]ithin the context of their own activities, avoid causing or contributing to adverse human rights impacts and address such impacts when they occur.”*

5.6. Section 3 states that enterprises should:

*“[s]eek 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 these impacts.”*

5.7. BT cannot avoid responsibility for human rights violations simply because the company does not directly carry out the drone attacks or choose the drone targets suggested by its surveillance probes. The commentary to section 3 explains that in order to meet the expectation in section 3, an enterprise would need to influence the entity actually causing the adverse impact to prevent or mitigate that impact. ‘Business relationships’ are said to include “relationships with business partners, entities in its supply chain and

*any other non-State or State entity directly linked to its business operations, products or services”.*

- 5.8. BT has a business relationship with the US government’s DISA through which it provided communications infrastructure at the heart of US drone operations. The company also has an ongoing business relationship with the intelligence agencies to provide covert surveillance probes.
- 5.9. The company has declined on multiple occasions to demonstrate any steps or due diligence efforts it has taken to prevent or mitigate the human rights violations this infrastructure supports, in which case Reprieve can only assume no such steps have been taken.
- 5.10. In fact, when Reprieve asked at the recent AGM whether the company’s compliance framework for human rights or the Board-level review of its human rights policy would address the US drones programme or the mass surveillance that enables drone targeting, BT explicitly indicated that it has not and did not have plans to do so.
- 5.11. Pursuant to section 5, enterprises should:
- “[c]arry 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”.*
- 5.12. The commentary to section 5 explains that this process entails *“assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses as well as communicating how impacts are addressed”*. Furthermore, it should be *“an ongoing exercise, recognizing that human rights risks may change over time as the enterprise’s operations and operating context evolve.”* It is also recommended that when enterprises identify through their human rights due diligence process or other means that they have caused or contributed to an adverse impact, they should *“have processes in place to enable remediation”*.
- 5.13. This section draws on the UNGP human rights due diligence provisions. The commentary to section 17 of those Principles explains that in meeting the due diligence requirements, businesses should *“identify general areas where the risk of adverse human rights impacts is most significant, whether due to certain suppliers’ or clients’ operating context, the particular operations, products or services involved, or other relevant considerations, and prioritize these for human rights due diligence”*. It is indisputable that BT’s contracts with the US government are for military purposes and its compliance with intelligence agency requests to violate the privacy rights of all of its customers should be considered high-risk from a human rights perspective, and so should be prioritized for scrupulous due diligence.
- 5.14. As noted above, BT has flatly refused to explain what due diligence it has carried out in relation to the Contract or to the mass surveillance programmes. The UK NCP should call upon the company to explain this, particularly after releasing a policy note on this particular due diligence issue.

5.15. Even if BT had agreed to overhaul its human rights framework or include its role in drones and mass surveillance in its policy review, it is clear that policies alone are inadequate to fulfil the requirement in section 3. Instead, specific action is necessary to prevent or mitigate specific risks of adverse human rights impacts linked to BT's business.

5.16. Section 6 states that enterprises should:

*“Provide for or co-operate through legitimate processes in the remediation of adverse human rights impacts where they identify that they have caused or contributed to these impacts.”*

5.17. The commentary to this section explains that when enterprises identify, through their human rights due diligence or other means, that they have caused or contributed to an adverse impact, they should have processes in place to enable remediation. Given that Reprieve has repeatedly brought the adverse impacts of drone strikes and mass surveillance to BT's attention, the company should now remediate these effects or at the very least articulate steps to assess its involvement.

5.18. Simply asserting that BT takes human rights very seriously and that the company follows all OECD guidelines should not be acceptable, particularly in light of BT's refusal to disclose any details of its due diligence efforts, along with its exclusion of what the company deems to be “political issues.” Combined with a policy of corporate apathy and wilful ignorance with regards to the use of its services in drone strikes and mass surveillance, it is astounding that BT continues to congratulate itself on using the “power of communications to make a better world.”<sup>24</sup>

## 6. Conclusion

6.1. After a full investigation, the UK NCP should ask BT to take the following steps to address its adverse human rights impacts:

- (i) Cease to provide services under the Contract;
- (ii) In the alternative, procure an amendment to the Contract such that BT's STM-16 may not be used for the transmission of any information supporting drone strikes in Yemen or any other territory where there is no declared armed conflict or for illegal mass surveillance purposes;
- (iii) Provide Reprieve with clear evidence documenting:
  - (a) BT's policy in relation to contracts for support of US counter-terror operations, particularly those related to the use of weaponised drones,

---

<sup>24</sup> BT Group plc, “Better Future Report 2014” (May 2014)  
[http://www.btplc.com/betterfuture/betterfuturereport/pdf/2014/Better\\_Future\\_report2014-complete\\_report.pdf](http://www.btplc.com/betterfuture/betterfuturereport/pdf/2014/Better_Future_report2014-complete_report.pdf).

including any risk assessment policy in respect of complicity in violations of international law;

- (b) The human rights due diligence carried out prior to entering into the Contract, as required by the OECD Guidelines; and
- (c) Any efforts made to seek to prevent or mitigate the adverse human rights impacts to which BT is contributing;
- (iv) Put in place appropriate mechanisms to mitigate and remedy the human rights violations in Yemen to which it has contributed; and
- (v) Issue a transparency report on the extent of BT's cooperation with intelligence agencies to facilitate mass surveillance of its customers and any due diligence efforts undertaken on this issue.

## 7. Supporting documentation

- Kristine M. Sturkie, "NEXCOM Provides Internet Service to Military Members at Camp Lemonnier", *America's Navy* (8 February 2011) [http://www.navy.mil/submit/display.asp?story\\_id=58448](http://www.navy.mil/submit/display.asp?story_id=58448).
- "Death From Afar", *The Economist* (3 November 2012) <http://www.economist.com/news/international/21565614-america-uses-drones-lot-secret-and-largely-unencumbered-declared-rules-worries>.
- Reprieve, "Complaint to the UK National Contact Point under the Specific Instance Procedure of the OECD Guidelines for Multinational Enterprises in respect of BT plc" (15 July 2013) [http://www.reprieve.org.uk/media/downloads/2013\\_07\\_15\\_PUB\\_Complaint\\_to\\_UK\\_NC\\_P\\_re\\_BT\\_plc.pdf](http://www.reprieve.org.uk/media/downloads/2013_07_15_PUB_Complaint_to_UK_NC_P_re_BT_plc.pdf).
- John Goetz & Frederik Obermaier, "Snowden enthüllt Namen der spähenden Telekomfirmen", *Süddeutsche Zeitung* (2 August 2013) <http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791>.
- James Ball, Luke Harding, & Juliette Garside, "BT and Vodafone among telecoms companies passing details to GCHQ", *The Guardian* (2 August 2013)
- Daniel A. Medina, "Yemeni man seeks answers in US over deadly drone strike." *Al Jazeera* (19 November 2013) <http://america.aljazeera.com/articles/2013/11/19/yemeni-activist-seeksanswersonusdronestrikethatkilledrelatives.html>.
- Mohammed al-Qawli, "The US killed by brother with a drone. I want to know why." *Al Jazeera* (5 December 2013) <http://america.aljazeera.com/opinions/2013/12/grieving->

yemena-sinnocentdead.html.

- Department of Defense, “Unmanned Systems Integrated Roadmap FY2013-2038” (23 December 2013) <http://www.defense.gov/pubs/DOD-USRM-2013.pdf>.
- UK NCP Review Committee, “Application for Review of the Initial Assessment – Recommendation of the Review Committee”, pp. 5-6 (17 January 2014)
- Jeremy Scahill and Glenn Greenwald, “The NSA’s Secret Role in the U.S. Assassination Program”, *The Intercept* (10 February 2014) <https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role>.
- Mark Ballard, “Telecoms Contractor Could be Called to Account for Drone Deaths”, *Computer Weekly* (21 March 2014) <http://www.computerweekly.com/blogs/public-sector/2014/03/telecoms-contractor-could-be-c.html>.
- BT Group, “Better Future Report 2014” (May 2014) [http://www.btplc.com/betterfuture/betterfuturereport/pdf/2014/Better\\_Future\\_report2014-complete\\_report.pdf](http://www.btplc.com/betterfuture/betterfuturereport/pdf/2014/Better_Future_report2014-complete_report.pdf).
- Mark Ballard, “Analysis: How the UK Connects to the US Global Drone Network,” *Computer Weekly* (2 May 2014) <http://www.computerweekly.com/news/2240220017/Analysis-How-the-UK-connects-to-the-US-global-drone-network>.
- Mark Ballard, “UK Telecoms Infrastructure Used to Support Controversial US Drone Operations”, *Computer Weekly* (2 May 2014) <http://www.computerweekly.com/news/2240219969/UK-telecoms-infrastructure-used-to-support-controversial-US-drone-operations>.
- Mark Ballard, “Analysis: How the UK Connects to the US Global Drone Network,” *Computer Weekly* (2 May 2014) <http://www.computerweekly.com/news/2240220017/Analysis-How-the-UK-connects-to-the-US-global-drone-network>.
- Lee Ferran, “Ex-NSA Chief: ‘We Kill People Based on Metadata’”, *ABC News* (12 May 2014) <http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata>.
- Duncan Campbell, “Revealed: GCHQ’s Beyond Top Secret Middle Eastern Internet Spy Base”, *The Register* (3 June 2014) [http://www.theregister.co.uk/2014/06/03/revealed\\_beyond\\_top\\_secret\\_british\\_intelligence\\_middleeast\\_internet\\_spy\\_base](http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base).
- Vodafone, Law Enforcement Disclosure Report (6 June 2014) <http://www.theguardian.com/business/2014/jun/06/vodafone-reveals-secret-wires->

allowing-state-surveillance.

- Mark Ballard, “Drone kill communications net illustrated”, *Computer Weekly* (13 June 2014) [http://www.computerweekly.com/cgi-bin/mt-search.cgi?blog\\_id=102&tag=HAIPE&limit=20](http://www.computerweekly.com/cgi-bin/mt-search.cgi?blog_id=102&tag=HAIPE&limit=20).
- Zoe Williams, “The new breed of shareholder activist: taking on the big boys at the AGM”, *The Guardian* (1 August 2014) <http://www.theguardian.com/business/2014/aug/01/new-breed-shareholder-activists>.