REPRIEVE

Complaint to the UK National Contact Point under the

Specific Instance Procedure of the OECD Guidelines for Multinational Enterprises:

British Telecommunications plc

10 October 2014

Contents

1. Summary of Complaint

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

- Facilitating the US drone programme by providing the Government Communications Headquarters (GCHQ) and the National Security Agency (NSA) with mass surveillance infrastructure. In exchange for tens of millions of pounds from these intelligence agencies, BT installs wiretaps on the United Kingdom's telecommunication cables and operates compromised optical fibre networks to enable the mass surveillance of global internet and phone traffic. Intelligence agencies openly acknowledge they rely upon this type of data to choose targets for drone strikes.

- Failing to provide evidence of due diligence mechanisms undertaken by the company to prevent the mass surveillance data from being used for targeting by unlawful US drone strikes in non-war zones.

2. Introduction

2.1. Reprieve is an international NGO that works to safeguard the human rights of people impacted by the counter-terrorism operations of the US and other governments.

2.2. 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.

2.3. Reprieve brings this complaint on behalf of its clients Mohammed al-Qawli and Faisal bin Ali Jaber, who have both lost family members to drone strikes guided by analysis of mass surveillance data. Reprieve originally brought the surveillance issue to the UK NCP's attention in a complaint dated 19 August 2014, which also addressed BT's construction of a fibre-optic cable at the heart of the "targeted killing" drone programme in Yemen and Somalia.[1] On 26 September 2014, the UK NCP requested that Reprieve submit a separate complaint that focused on BT's extensive collaboration in mass surveillance.

3. BT Plays Key Role in Mass Surveillance by Intelligence Agencies

3.1. BT does not publicly acknowledge the existence of a relationship or an agreement with GCHQ or the NSA. However, a significant amount of evidence indicates BT profits from a close collaborative business relationship with intelligence agencies.

3.2. In August 2013, *Süddeutsche Zeitung* and *The Guardian* revealed that BT has been working closely with the GCHQ to tap overseas communication cables and also to give the agency access to its customers' private communications without their knowledge or consent.[2] In turn, GCHQ was paid at least £100 million to share the intelligence with the NSA.[3] GCHQ's contribution to US intelligence is described as "significant" and the NSA's "closest ties are with the GCHQ".[4]

3.3. On 3 June 2014, *The Register* provided further detail about how BT "operate[s] extensive long distance optical fibre communications networks throughout the UK, installed and paid for by GCHQ, NSA, or […] NTAC".[5]

---

[1] 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) http://www.reprieve.org.uk/media/downloads/2014_08_19_INT_2nd_OECD_Complaint_re_BT.pdf.

[2] 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; 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.

[3] Nick Hopkins & Julian Borger, "Exclusive: NSA pays £100m in secret funding for GCHQ," *The Guardian* (1 August 2013) http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

[4] Ewan MacAskill & James Ball, "Portrait of the NSA: No detail too small in quest for total surveillance," *The Guardian* (2 November 2013) http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance.

[5] Duncan Campbell, "REVEALED: GCHQ's Beyond Top Secret Middle Eastern Internet Spy Base," *The Register* (3 June 2014)

3.4. While BT may contest whether its relationship with intelligence agencies goes beyond its obligations under UK domestic legislation, the company's complicity in mass surveillance is extremely profitable. In fact, BT and Vodafone were cited as the "two top earners of secret GCHQ payments running into tens of millions of pounds annually".[6]

3.5. Each time intelligence agencies "wanted to tap a new international optical fibre cable, engineers from 'REMEDY' [BT's codename] 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".[7]

3.6. This wiretapping occurs with such regularity that within GCHQ, BT has embedded groups of employees known as "Sensitive Relationship Teams" (SRTs). These secretive squads of BT staff are tasked with installing the software that stores customer data and funnels it into processing centres operated by intelligence agencies. The SRTs also install optical fibre "probes" into the equipment of other companies without their knowledge.[8]

3.7. Thus, BT provides an elaborate array of compromised cables, wiretaps, and hidden connections that feeds "much of the world's phone calls and internet data" to GCHQ headquarters in Cheltenham or to the agency's remote processing station in Cornwall.[9] In partnership with BT, GCHQ operates this "vast internet tapping operation" that allows the NSA to monitor "90% of the traffic crossing the UK". Each day, a quarter of all internet traffic in the world passes through the UK.[10]

3.8. To date, BT has declined to even issue a transparency report, as other telecommunications companies have done.[11] At its recent Annual General Meeting (AGM), BT publicly characterised its profound violations of privacy as a "political debate in which we don't engage."

3.9. At the AGM, Reprieve asked the company's board of directors whether BT planned to continue assisting intelligence agencies in intercepting the data used to carry out drone strikes. BT's response was its standard position of wilful 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."

3.10. When confronted with the extensive news stories of its complicity with mass surveillance and data retention, BT's final word was broadly dismissive: "[T]he

---

http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base.

[6] *Ibid*.

[7] *Ibid*.

[8] *Ibid.*

[9] Ball, *supra* note 2.

[10] MacAskill & Ball, *supra* note 4.

[11] Jennifer Rankin, "BT dismisses calls to reveal links to surveillance agencies," *The Guardian* (16 July 2014) http://www.theguardian.com/business/2014/jul/16/bt-dismisses-calls-reveal-links-surveillance-agencies.

media stories and speculation aren't necessarily anything we can use to change our position because it's not factual."

4. Mass Surveillance and Drone Strikes

4.1. Thanks to BT's well-paid assistance in tapping undersea cables, the NSA and GCHQ are able to vacuum up a vast amount of information about everyone in the world. A significant proportion of the data siphoned off to intelligence agencies is information about *how* we all communicate rather than *what* we communicate.[12]

4.2. In other words, while governments have made reassuring noises that "[n]obody is listening to your telephone calls" or reading our emails, intelligence agencies have been collecting vast amounts of data about when, where, and to whom we've been talking to.[13]

4.3. Commonly known as "metadata", this information *about* social media or phone activity reveals more about a person than one might expect, and it is actually easier for intelligence agencies to process than sifting through the actual content.[14]

4.4. In lieu of spending months reading emails or listening to phone calls, intelligence agencies can instead feed a targeted person's phone or email contacts into a computer. Within seconds, a computer shows an expansive network of the person's friends and acquaintances. When this is combined with additional data about everyone the person emails or chats with on Facebook and other social media, it *seems* to paint a picture about the beliefs, values, politics, and other aspects of life that most of us would rather keep private.[15]

4.5. In modern life, many people have hundreds if not thousands of interactions with different people. In this automated process, intelligence agencies rely upon assumptions about a person's friends and acquaintances that may turn out to be unwarranted.

4.6. BT's collaboration allows intelligence agencies to collect the massive amounts of private data required for the targeting. As the director of the Rand Center for Global Risk and Security describes the process, "[Intelligence agencies] collect stuff without

[12] John Naughton, "NSA surveillance: Don't underestimate the extraordinary power of metadata," *The Guardian* (21 June 2013) http://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama.
[13] *See, e.g.*, Michael Pearson, "Obama: No one listening to your calls," *CNN* (10 June 2013) http://edition.cnn.com/2013/06/07/politics/nsa-data-mining.
[14] *See* Mike Masnick, "Anyone Brushing off NSA Surveillance Because It's 'Just Metadata' Doesn't Know What Metadata Is," Tech Dirt (8 July 2013) https://www.techdirt.com/articles/20130708/01453123733/anyone-brushing-off-nsa-surveillance-because-its-just-metadata-doesnt-know-what-metadata-is.shtml.
[15] *See generally* John Naughton, "The NSA/GCHQ metadata reassurances are breathtakingly cynical," *The Guardian* (7 July 2013) http://www.theguardian.com/technology/2013/jul/07/nsa-gchq-metadata-reassurances.

knowing whether it's going to be relevant or not. We may find the answer before we know the question".[16]

Death by Unreliable Analysis

4.7. When used to compensate for poor military intelligence, this unreliable analysis presupposes guilt and regularly enables government-sanctioned murder. In February 2014, a former drone operator admitted the NSA identified people in Yemen, Somalia, and other countries for lethal drone strikes based simply on the target's mobile phone activity and location.[17]

4.8. In other words, intelligence agencies analyse a phone's activity for suspicious contacts and activity, rather than the actual content of calls. Drone strikes rely almost exclusively on these faulty assumptions in countries like Yemen where the US does not have a large presence on the ground.

4.9. As mass surveillance became an essential component of the US drones programme, 'We Track 'Em, You Whack 'Em' became the flippant motto within the NSA.[18] The former head of the NSA, General Michael Hayden, even explicitly stated that the US government kills people based on shaky analysis of mass surveillance data.[19]

4.10. The following cases illustrate the tragic consequences of relying on metadata for drone strikes:

Mohammed al-Qawli[20]

4.11. On 23 January 2013, Salim al-Qawli (Mohammed's cousin who worked as a taxi driver) picked up two paying customers in the village of Sinhan. Ali al-Qawli (Mohammed's brother who worked as a school teacher) was riding in the car as well.

4.12. When the taxi stopped at a military checkpoint, a US drone attacked the vehicle. The two taxi customers were likely identified as militants and deemed worthy of death by the US government. All four of the occupants of the vehicle were instantly killed. Initial reporting asserted that all four charred corpses in the taxi wreckage were suspected Al-Qaeda militants.[21]

---

[16] *See* Crofton Black, "Lifting the veil from Special Operations Command," *Al Jazeera America* (7 October 2014) http://america.aljazeera.com/opinions/2014/10/special-operationscommanddefensewarterrorappropriations.html.

[17] Jeremy Scahill & Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," *The Intercept* (10 Feb 2014) https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role.

[18] *Ibid*.

[19] 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.

[20] *See* Mohammed al-Qawli, "The US killed my brother with a drone. I want to know why", *Al Jazeera America* (5 December 2013) http://america.aljazeera.com/opinions/2013/12/grieving-yemena-sinnocentdead.html.

[21] *See, e.g.*, Associated Press, "US drone strike in Yemen kills suspected militants," *Fox News* (23 January 2013) http://www.foxnews.com/world/2013/01/23/us-drone-strike-in-yemen-kills-7-suspected-militants; Reuters, "U.S. drone kills six suspected al Qaeda members in Yemen – sources," (23 January 2013)

4.13. However, following the strike, an investigation by the Yemeni government determined that Ali al-Qawli and Salim al-Qawli "were not suspected of any crime nor linked to any terror organization".[22]

Faisal bin Ali Jaber[23]

4.14. Faisal bin Ali Jaber's relatives were similarly killed by drone strikes guided by poor intelligence. Salem bin Ali Jaber (Faisal's brother-in-law) was a respected local cleric who had delivered a strong sermon at the village mosque, decrying Al-Qaeda's extremism. On 29 August 2012, three unknown men arrived in the village and demanded to speak with Salem.

4.15. Salem was afraid that the trio were Al-Qaeda militants seeking retribution against him, so he asked his son Waleed bin Ali Jaber to accompany him while he talked with the men. Waleed and Salem met with the three men at a palm grove, and within seconds, four consecutive drone strikes devastated the area, killing the five men.

4.16. The mass surveillance programmes that BT facilitates and profits from are thus fundamentally flawed. The information gathered does not point conclusively to an individual. Instead, Hellfire missiles are locked onto a phone's SIM card in hopes that the person with the phone is a terrorist and that the phone's owner only associates with other terrorists.

5. **Breaches of the OECD guidelines**

5.1. BT collaborates with GCHQ and the NSA on a sprawling mass surveillance network that provides targets for unlawful US drone strikes in non-war zones.

5.2. BT violates the following provisions of the OECD Guidelines:

Chapter II (General Policies)

Chapter IV (Human Rights)

- *Paragraph 1 (Respect human rights)*
- *Paragraph 2 (Avoid causing or contributing to adverse human rights impacts)*
- *Paragraph 3 (Prevent or mitigate adverse human rights impacts that are directly linked to company via business relationship)*
- *Paragraph 5 (Carry out human rights due diligence)*

---

http://uk.reuters.com/article/2013/01/23/uk-yemen-qaeda-idUKBRE90M1HE20130123.

[22] Lotten Collin & Daniel Öhman, "Innocent people are killed in US drone attacks," *Sveriges Radio* (22 March 2013) http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5481640.

[23] *See* 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.

- *Paragraph 6 (Provide remediation of adverse human rights impacts where they identify that they have caused or contributed to these impacts)*

Chapter II, General Policies

5.3. 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"*.

5.4. In creating an extensive mass surveillance network for the US government's use in drone targetting, BT has demonstrated a complete failure to respect human rights.

Chapter IV, Paragraphs 1-3

5.5. Paragraph 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"*.

5.6. Paragraph 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"*.

5.7. Paragraph 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"*.

5.8. 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 wiretaps. The commentary to Paragraph 3 explains that an enterprise must attempt to influence the entity actually causing the adverse impact to prevent or mitigate that impact.

5.9. BT enjoys a close business relationship with GCHQ and the NSA. The company receives financial compensation for placing probes on fibre optic cables, and the company even embeds special teams within GCHQ.

5.10. The company has declined on multiple occasions to demonstrate any due diligence efforts it has taken to prevent or mitigate the drone strikes and other human rights violations this infrastructure enables, in which case Reprieve can only assume no such steps have been taken.

5.11. BT's refusal to produce a transparency report signals the company's unwillingness to even discuss its collaboration with intelligence agencies.

5.12. At its 2014 AGM, BT explicitly indicated that within its human rights compliance framework of the Board-level review of its human rights policy, it has not addressed—nor does it plan to—its involvement in mass surveillance which leads to murder by drone.

Chapter IV, Paragraph 5

5.13. Pursuant to Paragraph 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"*.

5.14. The commentary to Paragraph 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".

5.15. BT is regularly asked by intelligence agencies to breach the privacy of its customers and to insert wiretaps into communications lines. While this is a serious violation of privacy and human rights norms in itself, BT's partners also use the mass surveillance data to order the murder of innocent civilians. As detailed above, the information that BT funnels to UK and US intelligence agencies likely plays a key role in enabling unlawful US drone strikes.

5.16. BT has flatly refused to explain what due diligence it has carried out in relation to the mass surveillance programmes. Even if BT agrees to overhaul its human rights framework or include its role in drone warefare and mass surveillance in its policy review, policies alone are inadequate to fulfil the requirement in Paragraph 3. Instead, specific action is necessary to prevent or mitigate specific risks of adverse human rights impacts linked to the mass surveillance apparatus constructed by BT.

Chapter IV, Paragraph 6

5.17. Paragraph 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"*.

5.18. The Paragraph 6 commentary 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. BT's bland assertions that it takes human rights very seriously and that the company follows all OECD guidelines should not be acceptable, particularly in light of its refusal to disclose any details of its due diligence efforts and the company's exclusion of what it deems to be "political issues."

5.19. Given that Reprieve has repeatedly and publicly brought the adverse impacts of drone strikes and mass surveillance to BT's attention, the company should at least explain the extent of its complicity with GCHQ and the NSA.

6. **Objectives**

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

- Cease without delay its surveillance cooperation with the NSA and GCHQ
- Issue a transparency report on the company's role in partnering with intelligence agencies to create a mass surveillance programme.
- Disclose any due diligence efforts (if any) to assess BT's complicity in violations of international law and human rights, particularly with relation to mass surveillance enabling US drone strikes in non-war zones.

7. **Supporting Documentation**

- Associated Press, "US drone strike in Yemen kills suspected militants," *Fox News* (23 January 2013) http://www.foxnews.com/world/2013/01/23/us-drone-strike-in-yemen-kills-7-suspected-militants.
- Reuters, "U.S. drone kills six suspected al Qaeda members in Yemen – sources," (23 January 2013) http://uk.reuters.com/article/2013/01/23/uk-yemen-qaeda-idUKBRE90M1HE20130123.
- Lotten Collin & Daniel Öhman, "Innocent people are killed in US drone attacks," *Sveriges Radio* (22 March 2013) http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5481640.
- Michael Pearson, "Obama: No one listening to your calls," *CNN* (10 June 2013) http://edition.cnn.com/2013/06/07/politics/nsa-data-mining.
- John Naughton, "NSA surveillance: Don't underestimate the extraordinary power of metadata," *The Guardian* (21 June 2013)

http://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama.

- John Naughton, "The NSA/GCHQ metadata reassurances are breathtakingly cynical," *The Guardian* (7 July 2013) http://www.theguardian.com/technology/2013/jul/07/nsa-gchq-metadata-reassurances.

- Mike Masnick, "Anyone Brushing off NSA Surveillance Because It's 'Just Metadata' Doesn't Know What Metadata Is," *Tech Dirt* (8 July 2013) https://www.techdirt.com/articles/20130708/01453123733/anyone-brushing-off-nsa-surveillance-because-its-just-metadata-doesnt-know-what-metadata-is.shtml.

- Nick Hopkins & Julian Borger, "Exclusive: NSA pays £100m in secret funding for GCHQ," *The Guardian* (1 August 2013) http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.

- 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.

- 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.

- Ewan MacAskill & James Ball, "Portrait of the NSA: No detail too small in quest for total surveillance," *The Guardian* (2 November 2013) http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance.

- 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 my brother with a drone. I want to know why", *Al Jazeera America* (5 December 2013) http://america.aljazeera.com/opinions/2013/12/grieving-yemena-sinnocentdead.html.

- Jeremy Scahill & Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," *The Intercept* (10 Feb 2014) https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role.

- 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.

- Jennifer Rankin, "BT dismisses calls to reveal links to surveillance agencies," *The Guardian* (16 July 2014) http://www.theguardian.com/business/2014/jul/16/bt-dismisses-calls-reveal-links-surveillance-agencies.

- 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) http://www.reprieve.org.uk/media/downloads/2014_08_19_INT_2nd_OECD_Complaint_re_BT.pdf.

- Crofton Black, "Lifting the veil from Special Operations Command," *Al Jazeera America* (7 October 2014) http://america.aljazeera.com/opinions/2014/10/special-operationscommanddefensewarterrorappropriations.html.