EMBARGOED UNTIL 12PM GMT FEBRUARY 3RD 2013

Briefing note on OECD Complaints against Gamma International and Trovicor in the UK and Germany

Introduction

On 1st February 2013 Privacy International, together with fellow organisations, the European Centre for Constitutional and Human Rights ("ECCHR"), Reporters Without Borders, the Bahrain Center for Human Rights and Bahrain Watch, filed a complaint with the Organisation for Economic Cooperation and Development ("OECD") National Contact Point ("NCP") in the UK against Gamma International UK Ltd ("Gamma"), alleging that the company is in breach of the OECD Guidelines for Multinational Enterprises. A parallel complaint against Trovicor GmbH is being filed at the German NCP.

The complaints examine evidence indicating that Gamma and Trovicor have exported intrusive surveillance technology and training to Bahrain. By exporting surveillance technology to the Bahraini government, and are continuing to maintain these technologies for use by the Bahraini authorities, the complainants believe that this would make them culpable of aiding and abetting the Bahraini government in its perpetration of human rights abuses, including violation of the right to privacy, arbitrary arrest, torture, and suppression of free speech. In so doing, it is argued that the companies are in breach of several of the OECD Guidelines concerning human rights. In the case of Gamma, it is suggested that the example of Bahrain is illustrative of Gamma's more widespread practice of exporting surveillance technology to repressive regimes abroad.

Background on Gamma International and FinFisher

The complaint against Gamma is the latest in a series of attempts by Privacy International to halt the export of dangerous surveillance tools to abusive foreign regimes, where they are used to target political dissidents, human rights defenders, lawyers and journalists for arrest and torture. Privacy International is concerned about a number of UK surveillance vendors, but has focused on Gamma in particular over the past year due to the substantial evidence in the public domain concerning the use of the company's FinFisher products in repressive regimes across the Middle East, Africa and Central Asia.

Gamma's FinFisher suite is a particularly dangerous and sophisticated piece of surveillance technology: malware is sent to target individuals disguised as a harmless email, link (on a topic that is known to be of interest to the recipient) or software update (fake iTunes and Adobe

updates are common mechanisms of delivery), installs itself on the target's computer or phone device and relays information back to the sender, including the contents of all emails and Skype conversations, as well as address books and other data stored on the target's device. FinSpy can also be used to activate the device's internal camera and microphone and so capture images and audio recordings of the user. FinSpy is extremely difficult to detect, and thus an extremely potent weapon in the hands of oppressive regimes.

Media reports and expert testimony have strongly suggested that FinFisher products are or have been in use in dozens of countries around the world, including Egypt, Turkmenistan and Ethiopia, as well as in Bahrain[1]. With respect to Egypt in particular, the Guardian[2], the BBC[3] and Bloomberg News[4] have all reported that, in March 2011, documentation constituting an offer for sale of FinFisher was found in the ransacked headquarters of Mubarak's erstwhile intelligence agency, the State Security Investigations (SSI) service. According to a Bloomberg[5] news report, Martin J. Muench, the developer of FinFisher and Managing Director of Gamma International GmbH, has denied that a deal was ever finalised with Egypt.

Mr Muench has also repeatedly denied the veracity of findings by computer researchers at the University of Toronto, who have pinpointed FinSpy in over a dozen countries around the world, including Turkmenistan and Bahrain.[6] He maintains that Gamma has never done business with the government of Bahrain, but in August 2012 he claimed that a demo copy of FinSpy must have been stolen during a presentation via a USB stick and modified for use in Bahrain. The following day, researchers noticed that several of the pinpointed FinSpy servers were beginning to disappear. Servers in Singapore, Indonesia, Mongolia and Brunei went dark, while the Bahraini server briefly shut down before reincarnating elsewhere. Further analysis revealed that two different versions of FinSpy (believed to be versions 4.00 and 4.01) were used in Bahrain, which is inconsistent with the theory of a single stolen demonstration version. Both versions communicated with the same server in Bahrain. Furthermore, Bahrain's FinSpy server appeared to be receiving regular updates, most likely from Gamma.

---

[1] http://bits.blogs.nytimes.com/2012/08/13/elusive-finspy-spyware-pops-up-in-10-countries/

[2] http://www.guardian.co.uk/technology/2011/apr/28/egypt-spying-software-gamma-finfisher

[3] http://www.bbc.co.uk/news/technology-14981672

[4] http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html

[5] www.bloomberg.com/news/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy.html?allow_lang=en

[6] http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html?_r=2&

Background on Privacy International and Gamma International

On 12th July 2012 Privacy International initiated legal proceedings against the British government, sending a 'pre-action protocol' letter to the Department for Business Innovation and Skills ("BIS") calling for UK surveillance technology to be made subject to export controls. The letter contended that these surveillance products should be subject to the same export regime as that governing exports of military equipment, given that they have a comparable impact on the abuse and repression of citizens living under regimes. The letter focused on Gamma and its FinSpy products as exemplary of the type of company and surveillance software that are of concern.

BIS responded on 8th August 2012, in a letter stating that the Secretary of State for Business Innovation and Skills was not intending to broaden UK export controls legislation to include surveillance technology, although he was considering the possibility of international and/or EU-level agreement to further restrictions on the export of surveillance technology. Crucially, the letter confirmed that BIS had conducted an assessment of FinSpy and concluded that, because the products are designed to use controlled cryptography, they did fall within the scope of the existing export control regime (specifically under Category 5, Part 2 of Annex 1 to the Dual-Use Regulation) and thus required a licence for export. Privacy International responded to this letter on 9th August 2012, enquiring about the details of BIS's assessment and whether Gamma had sought any licences to export its FinFisher products, as it is required by law to do. BIS responded on 11th September 2012, stating that Gamma had not applied for or received any such licence.

On 9th November 2012, Privacy International wrote to Her Majesty's Revenue and Customs ("HMRC"), which is responsible for enforcement of the export regulations and policies set by BIS, and included a 186-page dossier of evidence concerning Gamma and its products. The letter stated that, if Gamma had continued to export FinFisher products to countries outside the EU without a licence, the company was acting in breach of UK export regulations and was thus engaged in criminal conduct. It also commented that, while Gamma has been exporting FinFisher since 2006, it had only submitted a Control List Classification request (the mechanism whereby companies ask HMRC whether or not their products require export licences) in July 2012. The letter requested a response within 14 days, but no conformation as to whether an investigation is taking place has been received.

Privacy International is still considering legal action against the British government for its failure to ensure effective oversight of exports of surveillance products from the UK. The OECD Guidelines for Multinational

Enterprises and the related complaint procedure provide a mechanism by which Privacy International, along with partner organisations, can address our concerns to the *companies* involved. The Guidelines are a series of recommendations setting forth principles and standards for responsible business conduct for multinational corporations operating in or from countries adhered to the OECD Declaration on International Investment and Multinational Enterprises (both the UK and Germany are adherents). We expect surveillance companies like Gamma International, who enjoy all the benefits of being headquartered in democratic countries where the rule of law is observed, to take steps to avoid facilitating the abuse and repression of less fortunate citizens around the world. We believe that Gamma should accept that their past failures in this respect has been unacceptable, and to put in place procedures to mitigate the harm already done, and avoid future harm, as a result of unethical exports of their products. We hope that the OECD Complaints procedure will bring this about.

Background on the OECD Guidelines for Multinational Enterprises

The OECD Guidelines for Multinational Enterprises is a key international instrument for promoting corporate social responsibility. The Guidelines are addressed by governments of adhering countries to enterprises that operate from or in those countries, and contain broad, non-binding recommendations for responsible business conduct, covering a range of issues such as labour, human rights, bribery, corruption and the environment. The role of the NCPs, which are created by, and based within, the governments of adhering countries, is to promote and implement the Guidelines, and, accordingly, they investigate complaints and provide a mediation and conciliation platform for resolving issues concerning the implementation of the Guidelines. If the NCPs accept the complaints against Gamma and Trovicor, they will proceed to investigate the extent of the defendant companies' complicity in human rights abuses in Bahrain, mediate between the complainants and defendants, and issue final statements concerning whether and which Guidelines have been breached.

The Complaints

The complaints outline: i) details concerning the defendant companies and their surveillance products, ii) the human rights situation in Bahrain, iii) evidence of use of surveillance products in Bahrain and their link to human rights abuses, and iv) violations of the OECD Guidelines.

i) The defendant companies and their technologies

Both Gamma and Trovicor manufacture and supply surveillance technology that can be used in relation to computers and mobile devices to intensively monitor communications, and store and analyse data.

Trovicor, a technology company that originally developed out of a business unit of Siemens and was owned by Nokia Siemens Networks until 2009, develops and supplies similar surveillance technologies, which are capable of analysing large amounts of data and tracking individuals via emails, fax, SMS, phone calls and bank transfer data. Trovicor's technology also supports the integration of trojans such as those developed by Gamma, and both Gamma and Trovicor refer to each other's products in their marketing materials.

ii) The human rights situation in Bahrain

Since the latter half of 2010 there has been a brutal crackdown on pro-democracy protestors in Bahrain, in the wake of pro-democracy uprisings across the Middle East. The complaints detail various repressive laws and practices in Bahrain, such as the restriction of press and internet freedom, the practice of torture, and the lack of due process and an independent judiciary. The complaints also detail Bahraini laws on communications surveillance, in particular the Lawful Access Regulation, which allows for intensive communications monitoring, as well as surveillance practices in Bahrain, which include heavy censorship of the internet and the frequent shutting down of websites that offend the government.

The report by the Bahrain Independent Commission of Inquiry ('BICI')[7], as well as reports by various human rights organisations, have established a clear connection between the suppression of free expression, systematic and widespread surveillance of telecommunications, and the arbitrary detention and torture of dissidents by the Bahraini government.

iii) **The evidence of use of surveillance products in Bahrain and their link to human rights abuses**

The complaints cite examples of Bahraini political activists who have been subject to communications monitoring, arbitrary arrest, and interrogation accompanied by torture. Both complaints cite the case of Abdul Ghani Al-Khanjar, a human rights activist who was arrested and tortured by Bahraini authorities in 2010, and who has stated that during his interrogation he was shown transcripts of text messages and mobile phone calls dating back to 2009. Mr Khanjar was unaware that government officials had access to these private communications.

The Gamma complaint examines the cases of three Bahraini human rights activists, Ala'a Shehabi, Husain Abdulla and Shehab Hashem, whose

[7] The report can be found at: http://www.bici.org.bh/BICIreportEN.pdf

computer and phone devices have been targeted by FinFisher spyware.[8] Ms Shehabi received emails on her computer in Bahrain in April and May 2012 that purported to contain news on topics concerning torture and prisoners. She did not open the links. Mr Abdulla received an attachment on the topic of human rights which was sent to his BlackBerry in May 2012 whilst he was in Washington DC. Mr Hashem also received emails on his computer in London in April and May 2012 that were identical to those received by Ms Shehabi.

The computer and mobile devices of these victims were subject to detailed study by security researchers Morgan Marquis-Boire at Citizen Lab (an interdisciplinary laboratory based at the Munk School of Global Affairs at the University of Toronto, Canada focusing on advanced research and development at the intersection of digital media, global security, and human rights)[9] and Bill Marczak from Bahrain Watch. Their research found the malware on the devices bore the hallmarks of FinFisher products: the computer code of the malicious programme contained multiple instances of the word 'FinSpy'. In addition, the security firm Rapid7 has conducted analysis based on the observation that an unexpected message ("Hallo Steffi") appeared when a user visited the internet address of Bahrain's FinSpy server in a web browser. They detected servers that responded in identical fashion in ten different countries, including the UAE, Qatar and Ethiopia.

Further scanning by Citizen Lab and Bahrain Watch has also confirmed servers in five additional countries (including Turkmenistan), as well as validating Rapid7's results.

iv) **Violations of OECD Guidelines**

The OECD Guidelines for Multinational Enterprises were first adopted by the OECD in 1976 and have been updated regularly since then, with seven editions in total. The two latest editions are the 2000 Edition (adopted on 27th June 2000) and the 2011 Edition (adopted on 1st September 2011). The main difference between these two is the inclusion in the 2011 Edition of a 'Human Rights' chapter and set of guidelines, which are lacking from the 2000 Edition.

Both the 2000 and 2011 Editions of the OECD Guidelines are examined in the complaints, due to the fact that the alleged breaches may have

---

[8] http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html

[9] CitizenLab expert reports can be found at: http://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/, and at: https://citizenlab.org/2012/08/the-smartphone-who-loved-me-finfisher-goes-mobile/

occurred both before and after September 2011, the date at which the 2011 Edition came into effect. In the case of Gamma, the maintenance and updating of the technologies, which are essential for the software's continued functioning and which are thus actions that constitute continued breaches of the Guidelines, have almost certainly been taking place since September 2011, and so engage the 2011 Edition of the Guidelines. However, the date at which the original supply took place has not been established, and so it is uncertain whether the 2000 or the 2011 Edition are engaged concerning this initial breach.

The 2011 OECD Guidelines identified as potentially being engaged are: Chapters II.A.2 and IV.1, which maintain that enterprises should respect internationally recognised human rights of those affected by their activities (both complaints identify arbitrary arrest, torture and extrajudicial killings as human rights abuses. The Gamma complaint focuses also on violation of the right to privacy as the right most directly caused by the company's malware products); Chapters II.A.11 and 12 and IV.2 and 3, which state that enterprises should try to prevent or mitigate adverse human rights impacts linked to their operations and products; Chapters II.A.10 and IV.5, which suggest that enterprises carry out due diligence, including human rights due diligence; Chapter II.A.13, which states that enterprises should encourage responsible business conduct by business partners; Chapter IV.4, which states that enterprises should have a human rights policy commitment; Chapter IV.6 which states that enterprises should co-operate in the remediation of adverse human rights impacts; and II. B. 1 which maintains that enterprises should support efforts to promote Internet Freedom. The 2000 OECD Guidelines identified as potentially being engaged are Chapter II.2 (equivalent to Chapter II.A.2 of the 2011 Edition, providing that enterprises should respect internationally recognised human rights of those affected by their activities), and Chapter III. 5, which states that enterprises should be encouraged to disclose certain information to the public, including their social and ethical policies, their systems for managing risks and complying with laws, and their statements or codes of business conduct.

The method of perpetration is identified in both complaints as complicity, which comprises the three elements of causation, knowledge and proximity. The complaints discuss how the companies have *caused* human rights abuses by enabling and/or exacerbating and/or facilitating the human rights abuses, how the companies *knew or should have known* of the likelihood that their products would result in human rights abuses, and how the companies were likely to have been *proximate* to the principal perpetrators both in time, space and relationship. The Gamma complaint specifies that even if the company is found not to be guilty of complicity, it still may have violated several OECD Guidelines.

The complaints end by outlining expectations towards both the defendant company and the NCP. It is expected that the defendant companies should

cease relations with Bahrain, implement a human rights policy and incorporate human rights due diligence into their operations, disclose contracts selling surveillance products to foreign governments, and remotely disable their products where they suspect they are being used to commit human rights violations. It is expected that the NCPs should investigate whether or not the defendant companies are involved in human rights abuses in Bahrain, issue final statements on whether OECD Guidelines have been breached, provide recommendations to the defendant companies on how to avoid further breaches of the Guidelines, and make follow-ups regarding the defendant companies' compliance with their recommendations.