IN THE INVESTIGATORY POWERS TRIBUNAL

BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Defendants

AMENDED STATEMENT OF GROUNDS

INTRODUCTION

1. The Claimants provide internet and communications services. They are referred to below as the "internet and communications service providers". They are based in various countries, including the UK. Collectively, they each provide a variety of services including internet access, email services, and website hosting.

    a. The First Claimant ("GreenNet") is a limited company active since 1986 and owned by the GreenNet Educational Trust, a charity registered in England & Wales.

    b. The Second Claimant ("Riseup") is a registered non-profit organisation based in Seattle, Washington, and active since 2000.

    c. The Third Claimant ("Mango Email Service") is a non-profit association in Zimbabwe and active since 1988.

    d. The Fourth Claimant ("Jinbonet") is a registered non-profit in South Korea, and active since 1988.

e. The Fifth Claimant ("Greenhost") is a company registered in the Netherlands and active since 2001.

f. The Sixth Claimant ("May First/People Link") is a registered non-profit organisation based in Brooklyn, New York and active since 2005.

g. The Seventh Claiminat ("Chaos Computer Club") is a registered non-profit organisation based in Hamburg, Germany, and active since 1981.

2. The Secretary of State for Foreign and Commonwealth Affairs is the minister responsible for oversight of the Government Communication Headquarters ("GCHQ"), the UK's signals intelligence agency.

3. These proceedings concern GCHQ's apparent targeting of internet and communications service providers in order to compromise and gain unauthorised access to their network infrastructures in pursuit of its mass surveillance activities. The claims set out below arise out of reports, published by the German newspaper *Der Spiegel*, that GCHQ has conducted targeted operations against internet service providers to conduct mass and intrusive surveillance.

4. In late 2013, *Der Spiegel* reported that GCHQ had attacked Belgacom, the Belgian telecommunications group, so as to enable it to engage in surveillance of users of Belgacom's network. The documents seen by *Der Spiegel* indicate that the attack "*was directed at several Belgacom employees and involved the planting of a highly developed attack technology referred to as a 'Quantum Insert' ('QI'). It appears to be a method with which the person being targeted, without their knowledge, is redirected to websites that then plant malware [malicious software] on their computers that can then manipulate them.*"[1] It is important to note that the employees of Belgacom were not targeted because they posed any legitimate national security concern. Instead, they were subject to intrusive surveillance because they held positions as administrators of Belgacom's networks. By hacking the employees, GCHQ could secure access to the customers. Once employees' computers were compromised, *Der Spiegel* reported, "*GCHQ continued to probe the areas of infrastructure to which the targeted employees had access […].*" Reportedly, GCHQ were "*on the verge of accessing the Belgians' central roaming*

[1] http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

router. The router is used to process international traffic. According to the presentation, the British wanted to use this access for complex attacks ("Man in the Middle" attacks) on smartphone users." A "Man in the Middle" attack is a technique for bypassing modern encryption software. It operates by interposing the attacker (here, GCHQ) between two computers that believe that they are securely communicating with each other. In fact, each is communicating with GCHQ, who collect the communications, as well as relaying them in the hope that the interference will be undetected.

5. *Der Spiegel* has further reported that the attack on Belgacom was "*not an isolated case, but in fact is only one of the signature projects of an elite British Internet intelligence hacking unit working under the auspices of a group called MyNOC*".[2] Indeed, *Der Spiegel* subsequently reported that GCHQ targeted internet exchange points run by German companies Stellar, Cetel and IABG. Reportedly, "*[t]he operation, carried out at listening stations operated jointly by GCHQ with the NSA in Bude, in Britain's Cornwall region, is largely directed at Internet exchange points used by the ground station to feed the communications of their large customers into the broadband Internet. In addition to spying on the Internet traffic passing through these nodes, the GCHQ workers state they are also seeking to identify important customers of the German teleport providers, their technology suppliers as well as future technical trends in their business sector.*"[3] It therefore appears that use is being made of this privileged access for the purposes of economic espionage, including economic espionage directed at other companies in the EU.

6. The Claimants are legitimately concerned about such attacks, of which they may have been, or may yet be, victims. The attacks gives rise to four main legal issues.

    a. First, in the course of such an attack, network assets and computers belonging to the internet and communications service provider are altered without the provider's consent. That is in itself unlawful under the Computer Misuse Act 1990 in the absence of some supervening authorisation. Depending on the nature and extent of the alterations, the attacks may also cause damage amounting to an unlawful interference with the internet and communications

[2] http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html
[3] http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html

service provider's property contrary to Article 1 of the First Protocol ("A1P1") to the European Convention on Human Rights ("ECHR").

b. Second, the surveillance of the internet and communications service provider's employees is an obvious interference with the rights of those employees under Articles 8 and 10 ECHR, and by extension the provider's own Article 10 rights. As *Der Spiegel* reported in relation to a separate attack on Mach, a data clearing company, a computer expert working for the company was heavily targeted: "*A complex graph of his digital life depicts the man's name in red crosshairs and lists his work computers and those he uses privately ('suspected tablet PC'). His Skype username is listed, as are his Gmail account and his profile on a social networking site. […] In short, GCHQ knew everything about the man's digital life*." It is not simply a question of GCHQ confining its interest to employees' professional lives. They are interested in knowing everything about the staff and administrators of computer networks, so as to be better able to exploit the networks they are charged to protect.

c. Third, the exploitation of network infrastructure enables GCHQ to conduct mass and intrusive surveillance on the customers and users of the internet and communications service providers' services in contravention of Articles 8 and 10 ECHR. Network exploitation of internet infrastructure enables GCHQ to undertake a range of highly invasive mass surveillance activities, including the application of packet capture (mass scanning of internet communications); the weakening of encryption capabilities; the observation and redirection of internet browsing activities; the censoring or modification of communications en route; and the creation of avenues for targeted infection of users' devices. Not only does each of these actions involve serious interferences with Article 8 ECHR rights, by creating vulnerabilities and mistrust in internet infrastructure they also chill free expression in contravention of Article 10 ECHR.

d. Fourth, the use by GCHQ of internet and communications service providers' infrastructure to spy on the providers' users on such an enormous scale strikes at the heart of the relationship between those users and the provider

itself. The fact that the internet and communications service providers are essentially deputised by GCHQ to engage in heavily intrusive surveillance of their own customers threatens to damage or destroy the goodwill in that relationship, itself an interference with the provider's rights under A1P1.

7. What is more concerning is that the conduct set out above has no proper justification. Each of the Claimants is a responsible and professional internet service provider. None has any interest in supporting terrorist activity or criminal conduct. They each comply with the law in the countries in which they operate, including UK law in the case of GreenNet, and US law in the case of RiseUp, and to the extent that access is legitimately required to user information held outside the UK, mutual legal assistance arrangements are available.

8. Articles 8, 10, and A1P1 to the Convention each impose requirements as to the nature of the legal justification for any interference. First, they require that the interference be "*in accordance with the law*", "*prescribed by law*", or "*subject to the conditions provided for by law*": in other words that there be a clear and ascertainable legal regime in place which contains sufficient safeguards against abuse of power and arbitrary use. Second, Articles 8 and 10 require that the interference be necessary in a democratic society and a proportionate means of achieving a legitimate aim; A1P1 requires that any deprivation of possessions be "*in the public interest*", which itself imposes a requirement of proportionality.

9. GCHQ has not identified any legal basis for the alleged conduct, which if performed by a private individual would involve the commission of criminal offences. It is assumed at this stage that the justification under domestic law is a warrant issued under s.5 Intelligence Services Act 1994 ("ISA 1994"), which permits *"entry on or interference with property or with wireless telegraphy"* in certain circumstances, and, to the extent that the relevant activities take place outside the British Islands, a warrant under section 7 of the Intelligence Services Act 1994 which purports to immunise from criminal liability "*any act done outside the British Islands, if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section…*".

10. Even if there is such an authorisation under sections 5 or 7 of the 1994 Act, it is nevertheless clear that (i) the interference with Convention rights is not "*in accordance*

with the law", "*prescribed by law*", or "*subject to the conditions provided for by law*", since such a warrant may not authorise certain types of CNE under domestic law, there is no adequate public legal regime in place that is capable of meeting those requirements, and (ii) it is not proportionate, both because of the extremely serious nature of the intrusions as against both the internet and communications service providers' employees and their users, and because the activity in pursuit of which the providers' infrastructure is manipulated (mass surveillance, censorship, redirection and modification, and the targeted infection of users' devices) appears to be indiscriminate in nature.

11. These grounds accompany the forms T1 and T2 filed by the Claimants and set out, in summary terms, the grounds relied upon. The Claimants will make detailed submissions and serve evidence in due course, once the Defendants have clarified the nature of their activities and their justification for them.

12. The Claimants also seek a public hearing of their complaint. The fact that documents evidencing the Defendants' activities have been released into and extensively reported on and analysed in the public domain means that there is no longer any good reason to uphold the Defendants' policy of 'neither confirm nor deny' in this case: see *R (Bancoult) v SSFCA* [2013] EWHC 1502 (Admin) at [28] and *CF v SSHD* [2014] EWCA Civ 559 at [20] per Maurice Kay LJ, Sullivan and Briggs LJJ agreeing: "*Lurking just below the surface of a case such as this is the governmental policy of "neither confirm nor deny" (NCND)... I do not doubt that there are circumstances in which the courts should respect it. However, it is not a legal principle. Indeed, it is a departure from procedural norms relating to pleading and disclosure. It requires justification similar to the position in relation to public interest immunity (of which it is a form of subset). It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it*".

THE DEFENDANTS' CONDUCT

13. From June 2013 onwards, a number of public disclosures have been made (beginning with publication in *The Guardian* and *The Washington Post* of documents leaked by a former NSA contractor, Edward Snowden) about programmes of surveillance operated by the NSA with the close involvement of other authorities, including the UK authorities and specifically GCHQ.

14. Many of the revelations concern the scope of the NSA and GCHQ's monitoring of communications, including the "*Prism*" programme (the monitoring of information stored by telecommunications companies or internet service providers) and "*upstream collection*" (the direct interception of communications during transmission). Those activities are the subject of existing complaints before the IPT.

15. This complaint relates to more recent revelations regarding GCHQ's intrusion into network infrastructures in order not only to monitor network traffic but also to use the networks to deploy malicious software ("malware") onto individual users' devices.

16. On 20 September 2013, *Der Spiegel* published an article entitled "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm." In that article it wrote:

> *"Documents from the archive of whistleblower Edward Snowden indicate that Britain's GCHQ intelligence service was behind a cyber attack against Belgacom, a partly state-owned Belgian telecoms company. A "top secret" Government Communications Headquarters (GCHQ) presentation seen by SPIEGEL indicate that the goal of project, conducted under the codename "Operation Socialist," was "to enable better exploitation of Belgacom" and to improve understanding of the provider's infrastructure.*
>
> *The presentation is undated, but another document indicates that access has been possible since 2010. The document shows that the Belgacom subsidiary Bics, a joint venture between Swisscom and South Africa's MTN, was on the radar of the British spies. […]*
>
> *According to the slides in the GCHQ presentation, the attack was directed at several Belgacom employees and involved the planting of a highly developed attack technology referred to as a "Quantum Insert" ("QI"). It appears to be a method with which the person being targeted, without their knowledge, is redirected to websites that then plant malware on their computers that can then manipulate them. Some of the employees whose computers were infiltrated had "good access" to important parts of Belgacom's infrastructure, and this seemed to please the British spies, according to the slides.*

The documents also suggest that GCHQ continued to probe the areas of infrastructure to which the targeted employees had access. The undated presentation states that they were on the verge of accessing the Belgians' central roaming router. The router is used to process international traffic. According to the presentation, the British wanted to use this access for complex attacks ("Man in the Middle" attacks) on smartphone users. The head of GCHQ's Network Analysis Centre (NAC) described Operation Socialist in the presentation as a 'success.'"

17. Subsequent disclosures, published by *The Intercept* on 12 March 2014, provide further information about the range of network exploitation and intrusion capabilities available to GCHQ. A joint presentation by GCHQ and NSA, entitled "Quantum Theory", depicts the process by which GCHQ exploited network infrastructure for targeted infection of users' devices.[4] The presentation clarifies that, rather than deploying Man in the Middle attacks, GCHQ and NSA employ a "Man on the Side" technique, which covertly injects data into existing data streams in order to create connections that will enable the targeted infection of users. The technique utilises an automated system – codenamed TURBINE. This system "*allow[s] the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually*," according to documents released by *The Intercept* on 12 March 2014.[5] Another undated document claims that TURBINE "*will increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants*."[6] Another document, shared with the Five Eyes surveillance alliance (i.e. including GCHQ), referred to TURBINE as permitting "*Industrial-scale exploitation*."[7]

18. In an article entitled "*How the NSA Plans to Infect 'Millions' of Computers with Malware,*" published on the same date, *The Intercept* details how GCHQ has worked closely with the NSA to develop implants, including "*An implant plug-in named CAPTIVATEDAUDIENCE, for example, is used to take over a targeted computer's microphone and record conversations taking place near the device. Another, GUMFISH, can*

[4] https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/
[5] https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/
[6] https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/
[7] https://firstlook.org/theintercept/document/2014/03/12/industrial-scale-exploitation/

covertly take over a computer's webcam and snap photographs. FOGGYBOTTOM records logs of Internet browsing histories and collects login details and passwords used to access websites and email accounts. GROK is used to log keystrokes. And SALVAGERABBIT exfiltrates data from removable flash drives that connect to an infected computer."

19. In addition to the above, GCHQ has developed extensive means of manipulating mobile devices. The means of compromising such devices, which are invariably internet-enabled, are likely similar if not identical to those of compromising any other computer. Documents published by *The Guardian* on 28 January 2014, in particular a set of slides from a GCHQ presentation delivered on 28 May 2010, revealed that GCHQ had by May 2010 developed a suite of software known as "WARRIOR PRIDE" for iPhones and Android devices, which appeared to allow at least for (i) the activation of a microphone and the taking of recordings without the user's consent ("Hot mic"), (ii) precise identification of the geographical whereabouts of the user ("High precision GEO"), (iii) avoidance of detection that the security of the device has been compromised ("Kernel stealth" and "Self-protection"), and (iv) the retrieval of any content on the phone.

20. In a further article on 11 November 2013 entitled "*GCHQ targets engineers with fake LinkedIn pages*", *Der Spiegel* elaborated on the mechanics of the attack on Belgacom. It described how GCHQ had targeted employees of Belgacom, subjected them to surveillance, and compromised their computers using malware. It also claimed that Belgacom was not the only company that had been targeted in this way.

> *"The Belgacom employees probably thought nothing was amiss when they pulled up their profiles on LinkedIn, the professional networking site. The pages looked the way they always did, and they didn't take any longer than usual to load.*
>
> *The victims didn't notice that what they were looking at wasn't the original site but a fake profile with one invisible added feature: a small piece of malware that turned their computers into tools for Britain's GCHQ intelligence service.*
>
> *The British intelligence workers had already thoroughly researched the engineers. According to a "top secret" GCHQ presentation disclosed by NSA whistleblower Edward Snowden, they began by identifying employees who worked in network*

maintenance and security for the partly government-owned Belgian telecommunications company Belgacom. […]

The computers of these "candidates" were then infected with computer malware that had been placed using infiltration technology the intelligence agency refers to as "Quantum Insert," which enabled the GCHQ spies to deeply infiltrate the Belgacom internal network and that of its subsidiary BICS, which operates a so-called GRX router system. This type of router is required when users make calls or go online with their mobile phones while abroad. […]

The operation is not an isolated case, but in fact is only one of the signature projects of an elite British Internet intelligence hacking unit working under the auspices of a group called MyNOC, or "My Network Operations Centre." MyNOCs bring together employees from various GCHQ divisions to cooperate on especially tricky operations. In essence, a MyNOC is a unit that specializes in infiltrating foreign networks. […]

In the case of Mach [a data clearing company which had also been targeted], the GCHQ personnel had "identified three network engineers" to target. Once again, the Quantum Insert method was deployed.

The spies first determine who works for a company identified as a target, using open source data like the LinkedIn professional social networking site. IT personnel and network administrators are apparently of particular interest to the GCHQ attackers, because their computers can provide extensive access privileges to protected corporate infrastructures. […]

In the case of Mach, for example, the GCHQ spies came across a computer expert working for the company's branch in India. The top-secret document shows how extensively the British intelligence agents investigated the life of the innocent employee, who is listed as a "target" after that.

A complex graph of his digital life depicts the man's name in red crosshairs and lists his work computers and those he uses privately ("suspected tablet PC"). His Skype username is listed, as are his Gmail account and his profile on a social networking site. The British government hackers even gained access to the cookies on the

unsuspecting victim's computers, as well as identifying the IP addresses he uses to surf the web for work or personal use.

In short, GCHQ knew everything about the man's digital life, making him an open book for its spies. […]

But that was only the preparatory stage. After mapping the man's personal data, now it was time for the attack department to take over. On the basis of this initial information, the spies developed digital attack weapons for six Mach employees, described in the document as "six targeting packs for key individuals," customized for the victims' computers. […]

Apparently, the agencies use high-speed servers located at key Internet switching points. When a target calls up a specific website, such as LinkedIn, these servers are activated. Instead of the desired website, they supply an exact copy, but one that also smuggles the government hackers' spying code onto the target computers.

According to other secret documents, Quantum is an extremely sophisticated exploitation tool developed by the NSA and comes in various versions. The Quantum Insert method used with Belgacom is especially popular among British and US spies. It was also used by GCHQ to infiltrate the computer network of OPEC's Vienna headquarters. […]

Much like the Belgacom spying operation, Wylekey is considered a great success. According to a summary, it provided GCHQ with detailed information about Mach, its communications infrastructure, its business profile and various key individuals."

21. A subsequent article published by Der Spiegel on 29 March 2014, "*'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel*," recounts a similar operation by GCHQ against German infrastructure companies Stellar, Cetel and IABG.

> "*Stellar operates a satellite ground station in Hürth, a so-called "teleport." Its services are used by companies and institutions; Stellar's customers include Internet providers, telecommunications companies and even a few governments […] Using their ground stations and leased capacities from satellites, firms like Stellar -- or competitors like Cetel in the nearby village of Ruppichteroth or IABG, which is*

headquartered in Ottobrunn near Munich -- can provide Internet and telephone services in even the most remote areas […]

The service they offer isn't just attractive to customers who want to improve their connectivity. It is also of interest to Britain's GCHQ intelligence service, which has targeted the German companies. Top secret documents from the archive of NSA whistleblower Edward Snowden viewed by SPIEGEL show that the British spies surveilled employees of several German companies, and have also infiltrated their networks.

One top-secret GCHQ paper claims the agency sought "development of in-depth knowledge of key satellite IP service providers in Germany."

The document, which is undated, states that the goal of the effort was developing wider knowledge of Internet traffic flowing through Germany. The 26-page document explicitly names three of the German companies targeted for surveillance: Stellar, Cetel and IABG.

The operation, carried out at listening stations operated jointly by GCHQ with the NSA in Bude, in Britain's Cornwall region, is largely directed at Internet exchange points used by the ground station to feed the communications of their large customers into the broadband Internet. In addition to spying on the Internet traffic passing through these nodes, the GCHQ workers state they are also seeking to identify important customers of the German teleport providers, their technology suppliers as well as future technical trends in their business sector."

22. Reportedly, GCHQ used similar tactics as with the Belgacom attack, targeting and monitoring employees, particularly engineers, as well as infiltrating and exploiting infrastructure. With respect to IABG, for example, *Der Spiegel* reported that the GCHQ document "*includes a list of IABG routers and includes their network addresses. In addition, it contains the email addresses of 16 employees at the company named as possible targets.*"[8]

23. Another NSA document, shared with GCHQ and published by *The Intercept* on 20 March 2014, describes in further detail how the employees of companies providing

[8] http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html

internet infrastructure services are "hunted" by NSA analysts. Employees performing system administration functions ("sys admins") are targeted by intelligence agents who, armed with the sys admin's work email, personal webmail or Facebook credentials can use Quantum to target that individual and subsequently gain access to the internet and communications service provider's entire network. In a post to an internal NSA forum entitled "*I hunt sys admins*", one agent describes the process as follows:

> "*Up front, sys admins generally are not my end target. My end target is the extremist/terrorist or government official that happens to be using the network some admin takes care of. Sys admins are a means to an end. For example, assume your target is using a CDMA device* [i.e. a mobile telephone] *on a foreign network: there may be situations where we passively collect his phone call/SMS out in the wild, but it would be* ***really*** *nice if we had access to the local infrastructure where we could monitor which tower he's connected to at any given point in time, or monitor all phone calls/data traffic that his phone generates. Many times, its difficult to directly target infrastructure… generally we'll need a fair amount of information going into an operation […] In order to get that, who better to target the person that already has the 'keys to the kingdom'? Many times, as soon as I see a target show up on a new network, one of my first goals is, "Can we get CNE access to the admins on that network, in order to get access to the infrastructure that target is using?"*

24. An excerpt from a further NSA document, published by *The Intercept* on 12 March 2014 makes the same point under the description "hacking routers".[9] The author writes:

> "*[…] let's go over some of the things that someone could do if they hack a router:*
>
> - *You could add credentials, allowing yourself to log in any time you choose*
> - *You could add/change routing rules*
> - *You could set up a packet capture capability… imagine running Wireshark on an ISP's infrastructure router… like a local listening post for any credentials being passed over the wire(!)*

[9] https://firstlook.org/theintercept/document/2014/03/12/five-eyes-hacking-large-routers/

- *You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels[…]"*

The author concludes: "*Hacking routers has been good business for us and our 5-eyes partners for some time now […]*".

25. It is not known (not least because there is no clear or accessible legal regime governing it) how many such attacks have been carried out, against whom, what damage has been caused to the targeted internet and communications service providers' systems, how many providers' employees have been specifically targeted and subjected to surveillance, how many users subjected to mass and intrusive surveillance and users' devices compromised as a result, who has access to the information collected as a result of all the above, for how long and on what terms. That is itself a significant cause for concern. But in any event there are two other concerns as a matter of principle.

    a. First, the process of exploiting an internet and communications service provider's infrastructure obviously involves a breaching the security of the infrastructure. It is therefore highly likely that any such breach compromises the security of the network going forward, leaving the infrastructure open to further damage or exploitation by a third party. For instance, the changes necessary to compromise the system may result in security vulnerabilities that could be exploited by third parties in other ways. As well as simply being a byproduct of compromising the network, the weakening of security may even be deliberate, as the reference in the document quoted at paragraph 24 above to "*weaken[ing] any VPN encryption capabilities on the router*" makes clear.

    b. Second, the tools allow GCHQ access to a large amount of highly private data pertaining to both an internet and communications service provider's employees and its users, including all individuals whose communications may pass through the internet and communications service provider's infrastructure. That is not only relevant to the level and proportionality of the interference with the rights of the internet and communications service providers' employees and users; it is also relevant to the impact on the internet and communications service providers' business due to the fact that

their systems are being used as a means of facilitating extremely intrusive surveillance of their own customers. On any view, GCHQ's interferences are of unprecedented scope and seriousness:

i. The information stored on a computer or mobile device is potentially far more comprehensive than the information that an individual communicates over a network in a manner capable of interception, or even information that could be obtained from a search of his home or office. These devices may contain not only details about the user's personal circumstances (for instance his age, gender, or sexual orientation), but also financial information, unencrypted passwords, privileged legal information and so on. Unlike in the case of an interception of communications, even information that the user deems too personal, private or sensitive to communicate is vulnerable to collection or monitoring when intrusion tools are utilised.

ii. Moreover, GCHQ's intrusive malware also appears to grant total control over the device, enabling the manipulation of functions including the camera and microphone without authorisation, and thereby the gathering of data which the user has never even chosen to store, let alone communicate to others.

iii. Finally, the intrusion is compounded by (a) the fact that, unlike in the case of a lawful search of a home or office, the user has little or no way of knowing that it has happened, and (b) compromised devices are likely to be left more vulnerable by virtue of the breaches necessary to enable the installation of the malware.

26. Further, there have been clear indications that GCHQ itself has reservations about the legality of such operations.

a. An undated NSA document referring to a trilateral programme between "*NSA, GCHQ, and FRA*" (the Swedish signals intelligence agency) for the deployment of the Quantum technique says: "*Continued GCHQ involvement*

may be in jeopardy due to British legal/policy restrictions".[10] There is no further explanation of the concerns.

b. A document prepared by a representative of GCHQ for an international telecommunications conference in September 2010 reads, in relation to the implanting of software to decrypt communications encrypted with a particular standard ("MIKEY-IBAKE"): "*An additional concern in the UK is that performing an active attack, such as the Man-in-the-Middle attack proposed in the Lawful Interception solution for MIKEY-IBAKE may be illegal. The UK Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material. A Man-in-the-Middle attack causes modification to computer data and will impact the reliability of the data. As a result, it is likely that LEMFs and PLMNs would be unable to perform LI on MIKEY-IBAKE within the current legal constraints.*"

Effect on the Claimants

27. In order to pursue this complaint, the Claimants need not show that they or their employees have actually been the subject of the alleged interference.

a. In the context of monitoring of communications, the European Court of Human Rights has held that "*the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under art.8, irrespective of any measures actually taken against them*": *Liberty v United Kingdom* (2009) 48 EHRR 1 at [56].

b. For the reasons given above, the interference in the present case is more serious than the monitoring of communications: it is the active manipulation

[10] https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html

of the internet and communications service provider's property, its employees and its users so as to enable the collection of data, including data which has never been communicated. Accordingly, the same principle applies in this case.

c. Likewise, if "*the mere existence of legislation*" permitting interference is a sufficient interference with a fundamental freedom to justify a legal challenge, then the fact that there is evidence of an interference without any meaningful legislative control is an even clearer case where a complainant need not show actual interference with his own affairs. In those circumstances, where there is no statutory scheme, Code of Practice or published policy indicating who can be targeted and in what circumstances, it is even more difficult for an individual to know whether they have been subject to the relevant activity.

d. Similarly, in the specific case of A1P1 and the effect on the internet and communications service providers' business dealings with their consumers, the very fact that there is an unconstrained prospect of the internet and communications service provider's network being used as a means of highly intrusive surveillance of its users damages the goodwill between the two, even if that surveillance is not in fact carried out.

28. The Claimants are clearly within the category of persons who may be affected by the interference; they, like Belgacom and the other companies known to have been affected, are providers of internet and communications services. Accordingly, the interference (i) affects the employees' personal data and impairs their freedom to communicate, (ii) in doing so, prevents the internet and communications service providers themselves from imparting and receiving information freely, and (iii) independently of that interference, it jeopardises the provider's relationships with its customers and potentially damages its property.

29. In fact, the Claimants are particularly susceptible to the A1P1 interference that will arise from destruction of or damage to customer goodwill, in that their brand profile is based to some extent a core belief in fundamental human rights and respect for the rule of law: their customer bases therefore consist in substantial part of individuals and organisations who have relied on those shared values to ensure their

communications are protected, and who are likely to be particularly concerned about mass and intrusive surveillance.

a. GreenNet advertises itself as "*the ethical Internet Service Provider that has been connecting people and groups who work for peace, the environment, gender equality and human rights since 1986*".

b. RiseUp advertises itself as providing "*online communication tools for people and groups working on liberatory social change. We are a project to create democratic alternatives and practice self-determination by controlling our own secure means of communications.*"

c. Jinbonet, the Korean Progressive Network, is described by the Association for Progressive Communications as an organisation that "*aims to support the growth of civil activity and communication by providing network services such as web hosting, community, e-mail, blog, progressive meta blog, mailinglist, etc to civil society organizations, trade unions, individuals and progressive projects*."

d. Greenhost advertises itself as offering "*a fresh approach to ICT and sustainability, and also supports various projects in the fields of education, culture and journalism. We are committed to a free and open internet and the security of our users.*"

e. May First/People Link describes itself as "*a politically progressive member-run and controlled organization that redefines the concept of "Internet Service Provider" in a collective and collaborative way*," and notes that its members are "*organizers and activists*."

f. Chaos Computer Club describes itself as a non-profit association with 3,600 members which "*[f]or more than thirty years [has been] providing information about technical and societal issues, such as surveillance, privacy, freedom of information, hactivism,* [and] *data security.*"

LEGAL FRAMEWORK

Human Rights Act 1998 and European Convention of Human Rights

30. By s.6 Human Rights Act 1998, it is unlawful for a public authority to act in a way which is incompatible with one of the rights set out in Schedule 1 to the Act, which incorporates various rights from the European Convention including Articles 8 and 10 and A1P1.

31. Article 8 of the Convention provides:

> 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> 2. *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 a democratic society in the interests of national security, public safety or the economic well-being 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.*

32. Article 10 provides:

> 1. *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> 2. *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

33. Article 1 of the First Protocol provides:

> "*Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public*

interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

34. The concept of 'possessions' in A1P1 covers all forms of property, including those which the applicant has only a legitimate expectation of receiving (*Kopecky v Slovakia* (2005) 41 EHRR 43). It has been held to include the goodwill or economic interests connected with the running of a business (*Tre Traktorer Aktiebolag v Sweden* (1989) 13 EHRR 309).

35. In *Hutten-Czapska v Poland* (2006) 42 EHRR 15 at 167-168, the Grand Chamber restated the principles governing justification of an interference with A1P1:

> "*Not only must an interference with the right of property pursue, on the facts as well as in principle, a 'legitimate aim' in the 'general interest', but there must also be a reasonable relationship of proportionality between the means employed and the aim sought to be realised by any measures applied by the state, including measures designed to control the use of the individual's property. That requirement is expressed by the notion of a 'fair balance' that must be struck between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights. The concern to achieve this balance is reflected in the structure of article 1 of Protocol No 1 as a whole. In each case involving an alleged violation of that article the court must therefore ascertain whether by reason of the State's interference the person concerned had to bear a disproportionate and excessive burden. […]In cases concerning the operation of wide-ranging housing legislation, that assessment may involve not only the conditions for reducing the rent received by individual landlords and the extent of the State's interference with freedom of contract and contractual relations in the lease market but also the existence of procedural and other safeguards ensuring that the operation of the system and its impact on a landlord's property rights are neither arbitrary nor unforeseeable. Uncertainty – be it legislative, administrative or arising from practices applied by the authorities – is a factor to be taken into account in assessing the State's conduct.*"

36. There are therefore four questions in any analysis of whether those rights have been breached:

    a. Is the relevant right engaged?

    b. Does the interference comply with the requirement of legal certainty imposed by the relevant Article?

    c. Is the interference in pursuit of a legitimate aim?

    d. Is the interference proportionate to the goal which is sought to be achieved (and, in the case of Articles 8 and 10, "*necessary in a democratic society*")?

Engagement of rights

37. Each of the rights is clearly engaged in the present case.

    a. As for Article 8, it is clear from the documents revealed by *Der Spiegel* that the employees targeted in the attack on Belgacom were subjected to deep personal surveillance. Even the GCHQ presentation (which appears to have been used for training purposes, and therefore with most of the relevant GCHQ staff having absolutely no need to know his personal information) made reference to an individual's name, a list of the computers he used at work and privately, his Skype username, his Gmail account, a social networking profile belonging to him, his IP addresses and the cookies on his computers (As *Der Spiegel* reported: "*In short, GCHQ knew everything about the man's digital life*"). This information appears to have been widely disseminated within GCHQ. All of those things are obviously private information within the meaning of Article 8. By way of example, the European Court of Human Rights has held in the context of workplace monitoring that that "*emails sent from work*" and "*information derived from the monitoring of personal internet usage*" are both protected by Article 8: Copland v United Kingdom (2007) 45 EHRR 37 at [41].

    b. The Article 8 rights of the internet and communications service providers' users are also affected by GCHQ's conduct. Exploitation of the internet and communications service providers' infrastructure enables GCHQ to conduct

surveillance on users of the providers' services, either through mass monitoring or filtering of communications, or through the targeted infection of users' devices with malware.

c. As for Article 10, the Court has recognised in *Weber* (above, [144-145]) that the fact that "*the threat of secret surveillance […] necessarily strikes at the freedom of communication of users of telecommunications services*" means that it engages Article 10 if the effect is to discourage communications. The same principle must apply to the threat of intrusion into computers and devices via the internet, to the extent that it discourages the free use of the internet, which it obviously will if left uncontrolled.

d. As for A1P1, (i) to the extent that the internet and communications service providers' computers and network assets have been damaged or materially altered in the course of such an attack there will obviously be an interference with its property, and (ii) in any event, the unauthorised deputisation of the internet and communications service provider to assist GCHQ in spying on its customers will have an obviously detrimental effect on the provider's commercial relationships and the goodwill it enjoys, which is a 'possession' within the meaning of A1P1 as set out above.

Legal certainty

38. It is well settled that the requirements set out in Articles 8 and 10, that the interference be "*in accordance with the law*" or "*prescribed by law*", demand more than merely that the interference be lawful as a matter of English law: it must also be "*compatible with the rule of law*": *Gillan v United Kingdom* (2010) 50 EHRR 45 at [76]. That means it must "*afford a measure of legal protection against arbitrary interferences by public authorities*", and indicate "*with sufficient clarity*" the scope of any discretion conferred and the manner of its exercise: *Gillan* at [77].

39. Although the text of A1P1 only provides expressly that any deprivation of possessions must be "*subject to the conditions provided for by law*", the same principle applies equally to interferences with possessions. In *Amat-G Ltd v Georgia* (2007) EHRR 35, the ECtHR held at [58-61] that an interference which was neither a deprivation nor a control of use could nevertheless only be lawful if it "*satisfied the*

requirement of lawfulness and was not arbitrary", stating that "*the rule of law, one of the fundamental principles of a democratic society, is inherent in all provisions of the Convention*". The three Articles may therefore be treated as identical for the purposes of this criterion.

40. Numerous cases have addressed this requirement in the context of secret surveillance and information gathering.

    a. In Malone v United Kingdom (1985) 7 EHRR 14, the Court held that the legal regime governing interception of communications "*must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*" [67]. It must be clear "*what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive*" and the law must indicate "*with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities*" [79].

    b. In Association for European Integration and Human Rights v Bulgaria (62540/00, 28 June 2007), the Court held at [75]: "*In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for us is continually becoming more sophisticated […]*".

    c. These requirements apply not only to the collection of material, but also to its treatment after it has been obtained, including the "*procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material*" (Liberty v UK (2009) 48 EHRR 1 at [69]).

    d. In Weber the ECHR held at [93-94]: "*The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures […] Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion*

granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

e. The Court continued in *Weber* by setting out the matters which any legal regime governing secret surveillance must expressly address in statute in order to be regarded as lawful:

> *95 In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.*

Legitimate aim and proportionality

41. The Claimants accept that, in principle, surveillance may be conducted for legitimate aims such as national security. As set out in more detail below, they deny that the interference in this case is a proportionate means of achieving such a legitimate aim.

<u>*Domestic legal regime governing the relevant conduct*</u>

Regulation of Investigatory Powers Act 2000

42. RIPA 2000 regulates, among other things, the interception of communications in the course of transmission (Part I Chapter I), the acquisition of communication data from persons providing a telecommunication service (Part I Chapter II), and intrusive surveillance and covert human intelligence sources (Part II), in the UK.

43. Part I Chapter I empowers the Secretary of State to issue warrants for the interception of communications under s.5, if he considers the interception necessary

on a number of listed grounds, including national security, and proportionate to the aim to be achieved.

44. Section 2(2) RIPA 2000 defines "*interception*" as follows:

> "*a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he –*
>
> > *(a) so modifies or interferes with the system, or its operation,*
> >
> > *(b) so monitors transmissions made by means of the system, or*
> >
> > *(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,*
>
> *as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.*"

45. That might extend to some of the effects of the conduct at issue in this complaint – for instance, if malware were implanted and then used in order to record a phone call while it is being made – but it does not cover most of the functions described in the leaked documents. For example, the extraction of documents from a hard disk or a mobile device would not be the interception of a communication in the course of its transmission; it might involve the collection by GCHQ of information which the affected individual never intended to share with anyone. Likewise, the ability to activate a user's camera or microphone without his knowledge would not involve the interception of any communication. Accordingly, it cannot be said that the implanting of malware is merely a modification "*so […] as to make some or all of the contents of the communication available while being transmitted*".

46. RIPA Part I Chapter II covers the acquisition and disclosure of "*communication data*", namely data held by a person providing a telecommunication service (section 21(4)). That is clearly not engaged.

47. Part II is not engaged either; s.48(3) provides that "*References in this Part to surveillance do not include references to […] (c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorised under – (i) section 5 of the*

Intelligence Services Act 1994 […]". In a case involving interference with property by GCHQ, which (as set out below) is governed by the Intelligence Services Act 1994, that exemption applies. In any event, nowhere in Part II is there any reference to the manipulation of electronic devices belonging to others; the Act is clearly aimed at a different kind of information-gathering, its interpretation provisions referring to "*monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications*", either by officials alone or "*by or with the assistance of a surveillance device*" (s.48(2)), and only in certain circumstances "*the interception of a communication in the course of its transmission*". As an interference with fundamental rights it cannot lightly be construed as covering an entirely different kind of information-gathering: *R (Simms) v SSHD* [2000] 2 AC 115. In any event, it does not even arguably extend to activity such as the collection and extraction of documents.

Computer Misuse Act 1990

48. It is an offence under s.1(1) Computer Misuse Act 1990 ("CMA 1990") to cause a computer to perform any function with intent to secure access to any program or data held in it, or to enable any such access to be secured, if the access is unauthorised and known to be unauthorised. (The term "*computer*" is not defined in the Act, but in another statutory context was held by Lord Hoffmann in *DPP v McKeown* [1997] 1 WLR 295 to mean "*a device for storing, processing and retrieving information*". Modern mobile devices, which are far more sophisticated and powerful than the desktop computers available when the Act was passed, undoubtedly qualify.)

49. Further, under s.3 CMA 1990 it is an offence to do any unauthorised act in relation to a computer, in the knowledge that it is unauthorised, if (i) the intention is to impair the operation of the computer, to prevent or hinder access to any program or data, to impair the operation of any program or the reliability of any data, or to enable any of those things, or (ii) the perpetrator is reckless as to whether the act will do any of those things. S.3(5) clarifies that the relevant effects may be only temporary, and also that a reference to doing an act includes a reference to causing an act to be done. The result is that the infection of a computer pursuant to an automated process would still be an offence on the part of the person who commenced or directed that process. The intrusion at issue here not only impairs the operation of the target computers in

multiple ways, including by draining battery life and using bandwidth and other computer resources, undermining security features such as encryption and intrusion prevention. The intrusion also impairs the actual network infrastructure owned and operated by the internet and communications service providers, and the services and programs run on the infrastructure.

50. S.10 CMA 1990 provides that section 1(1) "*has effect without prejudice to the operation (a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and (b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure*." However, this override does not apply to section 3(1). Therefore, at least to the extent that such activities occur in England and Wales, any GCHQ activities that impair the operation of a computer – for instance, by leaving it vulnerable to future exploitation, as explained above are *prima facie* unlawful.

Intelligence Services Act 1994

51. S.3 ISA 1994 provides the statutory basis for GCHQ and delineates its statutory functions. Those functions include "*to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide [to various organisations] information derived from or related to such emissions or equipment and from encrypted material*". By s.3(2) those functions are exercisable only in the interests of national security, the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands, or in support of the prevention or detection of serious crime.

52. S.4(2) requires the Director of GCHQ to ensure "*that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings*."

53. S.5(1) provides: "*No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section*." The Secretary of State may issue such a warrant on the application of GCHQ in respect of any action, provided he "*thinks it necessary for the action to be taken for the purpose of assisting […] GCHQ in carrying out [its statutory functions],*" "*is satisfied that the taking of the action is proportionate to what the action seeks to achieve*", and is satisfied

that satisfactory arrangements are in force with respect to section 4(2) in relation to onward disclosure.

54. In other words, the apparent legal basis for the activity at issue in this complaint is an extremely broad power on the part of the Secretary of State to render lawful what would otherwise be unlawful.

GROUND 1: IN ACCORDANCE WITH LAW / PRESCRIBED BY LAW

55. As already indicated, there are three types of activity at issue in this complaint. The first relates to the manipulation of the targeted internet and communications service providers' property and the unauthorised changes made to its assets and infrastructure. The second and third relate to the surveillance of the internet and communications service providers' employees and customers respectively.

56. Together they form part of a covert and potentially enormous programme of surveillance which has only come to light as a result of unauthorised disclosures. The nature of that programme of surveillance, under which internet and communications service providers, their employees or their customers may have no idea they have even been subjected to it, is such that it cannot possibly be Convention-compliant in the absence of a clear legal framework governing its use.

    a. The surveillance which it is aimed at facilitating has the potential to be more intrusive than any other form of surveillance or data-gathering. The amount of information stored on mobile phones and computers is vast, and much of it will be highly personal in nature. Unlike the monitoring of communications, these activities enable GCHQ to obtain that information whether or not the affected individual has ever chosen to share it with anyone.

    b. Moreover, the logging of keystrokes and the covert activation of cameras and microphones enable GCHQ to obtain further potentially sensitive information whether or not the affected individual has ever chosen even to store it.

    c. A user may not even know of the full extent of what his computers or mobile devices store. A mobile phone may, for instance, log all his historical

geographical movements as well as his current location. For instance, if he went for a job interview or a medical appointment during work hours, that would be logged regardless of whether there were any other record of that interview or appointment having been arranged.

d. The fact that computers and devices are vulnerable to intrusion in this way will inevitably discourage people from using the internet freely.

e. The potential vulnerabilities resulting from the forcible infection of devices and the necessary weakening of security that such manipulation involves have the potential to produce further interferences beyond those which GCHQ directly controls.

f. The potential for GCHQ to take over a compromised device altogether, potentially altering its contents, raises serious concerns about the integrity of any evidence from such sources that might be used in legal proceedings, and the mechanisms would should be established and enforced in order to ensure that that integrity is protected.

g. As a matter of general principle, the fact that computer hacking involves sophisticated technology and concepts which were unknown 20 years ago strongly militates in favour of a requirement that it be governed by an appropriate legal framework developed with that technology and those concepts in mind.

57. Accordingly, it is if anything more necessary than in an ordinary 'interception' case that there be a clear legal framework governing activities of this sort.

58. There is no such framework. The only statutory scheme dealing expressly with the unauthorised infection of computers was established in 1990. Far from establishing a Convention-compliant framework within which such infection is to be permissible on certain conditions and with certain safeguards, it makes clear that GCHQ's activity is simply unlawful in the absence of a supervening provision. The availability of a warrant under ISA 1994 that simply cancels any unlawfulness is self-evidently not an adequate safeguard.

59. There is no Code of Practice governing the circumstances in which intrusion will be permitted, by what means, against whom, in response to what level of suspicion and for what kind of misconduct, or for how long their systems will be permitted to remain compromised. Nor is there anything governing the procedure to be followed in selecting for examination, sharing, storing and destroying any material obtained (*Liberty* at [69]), or anything governing the relationship between GCHQ's programme and the equivalent programmes being pursued by the NSA, FRA, and potentially others. Even if it is strictly speaking permissible as a matter of construction of domestic law (which, given the Defendants have not yet advanced any such case, is not admitted), it falls short of the requirements of the rule of law and of the various articles of the Convention which import those requirements.

GROUND 2: DISPROPORTIONALITY OF INTERFERENCE

60. Given the limited availability of the details of GCHQ's activity (still less the purported legal basis for it) to the Claimants at this stage, the Claimants must reserve the right to make more detailed submissions on the disproportionality of the interference in due course.

61. For present purposes it is sufficient to say:

    a. As set out above, the nature of the intrusion carried out against internet and communications service providers' employees and customers is far more serious than the interception of their communications and, if left unchecked, amounts to one of the most intrusive forms of surveillance any government has ever conducted. The amount of data which can be collected, and the speed, ease and surreptitiousness with which it can be done, is completely unprecedented. In those circumstances any such intrusion would have to be highly targeted and justified by very specific circumstances in order for the activity to be proportionate to any legitimate aim.

    b. All the indications so far are that the activity goes far beyond any such specific justification. Indeed, the compromising of network infrastructures would tend to suggest the opposite: as reported by *The Intercept* in March 2014, the NSA (with the cooperation of GCHQ) intends to use those infrastructures to deploy malware into "*millions*" of devices.

c. Moreover, the lack of safeguards mentioned above – in particular the apparent lack of any restriction on the extent or duration of the infection of any particular device – tends strongly against any finding that the interference is proportionate to any legitimate aim.

d. There is nothing in the publicly available documents relating to the attack on Belgacom which suggests that there was any specific justification for targeting Belgacom in particular, other than the fact that it was an operator of major network infrastructure and that this would enable the infection of its users' devices.

CONCLUSION

62. The Claimants therefore seek the following orders (which, again, may have to be supplemented or amended in light of further disclosures):

a. A declaration that GCHQ's intrusion into the computers and network assets of internet and communications service providers, their staff and their users is unlawful and contrary to Articles 8 and 10 and A1P1 ECHR;

b. An order requiring the destruction of any unlawfully obtained material;

c. An injunction restraining further unlawful conduct.

63. The Claimants adopt and support, *mutatis mutandis*, the amendments made in the *Privacy International* claim.

Ben Jaffey
Tom Cleaver
Blackstone Chambers

July 2014
Ben Jaffey
Tom Cleaver
Blackstone Chambers

19 May 2015