IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/15/110/CH**

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT

(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS

(4) SECURITY SERVICE

(5) SECRET INTELLIGENCE SERVICE

Respondents

WITNESS STATEMENT OF DR GUS HOSEIN

I, Dr GUS HOSEIN, Executive Director, Privacy International, 62 Britton Street, London EC1M 5UY SAY AS FOLLOWS:

1. I am the Executive Director of Privacy International. I have a B. Math (Hons) in Applied Mathematics with a minor in Computer Science from the University of Waterloo, Canada (1996)). I have an MSc in Information Security from the University of London (1997) and a PhD in Information Systems, focusing on cryptography, technology law and policy. I have advised government departments and international organisations on security and privacy issues. I lead the Privacy International Technical Team, that includes two system administrators who are developing systems for deployment in hostile environments, particularly for our partner organisations in the Global South.

2. I am experienced in the development and deployment of computer networks (albeit not on the scale of those operated by GCHQ). I act as a system administrator for PI's computer systems.

3. The Claimant notes that the Respondents seek to distinguish various techniques from their definition of Artificial Intelligence. I agree that there is no consensus on a definition of Artificial Intelligence. However, it is commonly understood to refer to

techniques from rule-based expert systems[1], fuzzy expert systems[2], frame-based expert systems[3], neural networks[4], evolutionary computation[5], hybrid intelligent systems[6], knowledge engineering[7], data mining and knowledge discovery[8]. Even if the Respondents seek to distinguish these from their own definition of Artificial Intelligence, and exclude use of algorithms and automated decision making, it does not appear from the evidence I have seen that *any* of these techniques have been subject to meaningful or technically informed independent oversight.

Systems administrators

4. The various errors in GCHQ's evidence will be the subject of submissions. In particular, it is both important and surprising that GCHQ contended that contractors had no access to operational systems, but then recanted that evidence and admitted that over 100 contractors have such access.

5. If senior GCHQ staff (up to and including the Deputy Director of GCHQ responsible for Mission Policy) had no idea that contractors within GCHQ had system administrator rights (indeed thought the very opposite of the true position), the oversight bodies would presumably not have known this information. This role of industry within GCHQ were not subject to independent oversight.

---

[1] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 52 *"A rule-based expert system has five basic components: the knowledge base, the database, the interference engine, the explanation facilities and the user interface."*

[2] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 125 *"Fuzzy logic is a logic that describes fuzziness. As fuzzy logic attempts to model humans' sense of words, decision making and common sense it is leading to more human intelligent machines."*

[3] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 162 *"A frame contains knowledge of a given object."*

[4] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 212 *"Artificial neural networks consist of a number of very simple and highly connected processors, called neurons, which are analogous to the biological neurons in the brain."*

[5] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 254 *"The evolutionary approach to artificial intelligence is based on the computational models of natural selection and genetics known as evolutionary computation. Evolutionary computation combines genetic algorithms, evolution strategies and genetic programming."*

[6] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 296 *"Hybrid intelligent systems are systems that combine at least two intelligent technologies; for example a combination of a neural network and a fuzzy system results in a hybrid neuro-fuzzy system."*

[7] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 358 *"Knowledge engineering is the process of building intelligent knowledge-based systems. There are six main steps: assess the problem; acquire data and knowledge; develop a prototype system; develop a complete system; evaluate and revise the system; and integrate and maintain the system."*

[8] Michael Negnevitsky, Artificial Intelligence, Addison Welsley, Third Edition, page 418

6. Below, I deal with the factual assertions made in GCHQ's evidence and give some context about the nature of systems administration.

7. To administer operational systems is to have full control over them and have privileged access to them. As one author in the area writes: "*Operating systems which restrict user privileges need an account which can be used to configure and maintain the system. Such an account must have access to the whole system, without regard for restrictions. It is therefore called privileged account ... These accounts place virtually no restriction on what the account holder can do. In a sense, they provide the privileged user with a skeleton key, a universal pass to any part of the system.*"[9]

8. The risks involved with the use of systems administrators with privileged access are well understood. Mr Snowden used such access to remove large quantities of UK TOP SECRET STRAP information when working as a NSA external contractor in Hawaii from GCHQ. He was not detected at the time. Given the numbers of people with similar access worldwide, it would be surprising if some had not misused their access for selfish purposes instead, such as for personal reasons or financial gain.

9. In October 2017 it was reported that an NSA contractor leaked US hacking tools by mistake to Russian cybersecurity firm Kaspersky Lab. The NSA contractor appears to have claimed to have taken NSA hacking software home to work on, using his home computer. According to Kaspersky, the contractor's home computer had its software installed. It detected a piece of malware attributed to "Equation Group" (the security firm's internal codename for what is believed to be the NSA's hacking team) on 11 September 2014. It then uploaded the relevant software, including its source code to Kaspersky, believing it to be malware worthy of analysis and investigation. Whether Kaspersky's account is entirely accurate is much debated. An alternative explanation might be that Kaspersky was actively seeking to obtain secret information from the NSA. Alternatively, it is possible that the contractor was intending to leak information and did so via uploading it onto his home computer to give a plausible excuse for his conduct. Either way, this is a further example of a contractor acting in an unauthorized manner, even if not malicious.

10. Turning to the potential for malicious actors. In the case of GCHQ contractors, they not only test and maintain the systems but also developed the hardware and software, thus have an intimate knowledge of the ways the systems work. This represents a significant risk:

> "Inside knowledge draws emphasis to those mission-critical positions within the enterprise where a staff member's (or contractor's) access combined with their knowledge of the systems and vulnerabilities, creates the greatest potential for harm from an insider attack. For instance, despite technical advances, the greatest potential risk factor that still remains is the staff member with access to high-level system privileges. This staff member may or may not have malicious intent and due to the rapid evolution of increasingly mobile and decentralized

[9] Aeleen Frisch, O'Reilley & Associates Inc, Essential System Administration, December 1995, page 5.

control access, he need not be physically located with the traditional data centre. Thus, the risk can exist both internally and externally to the enterprise."[10]

11. It is confirmed by Exhibit GCHQ 14 that:

> "1. Privileged Users for the purposes of this policy are those individuals who have IT system privileges that enable them to **by-pass some or all of the controls that govern the access and activity of normal users.** The extent of additional privilege ranges from those who have very limited additional privilege to execute specific tasks, those with additional privileges within an application, through those with full control or "system admin" or "root" accounts.

(emphasis added)

12. A system administrator or root account user may "*have complete control over systems and applications*"[11]. For example, "*On a UNIX system, the superuser is a privileged account with unrestricted access to all files and commands. The username of this account it root. Many administrative tasks and their associated commands require superuser status.*"[12]

13. It is crucial to limit the number of people with access to live systems, and to separate those responsible for development and testing:

> "One really important aspect of internal control in banking – and in systems generally – is to minimise the number of 'sysadmins', that is, of people with complete access to the whole system and the ability to change it. For decades now, the standard approach has been to keep development staff quite separate from live production systems. A traditional bank in the old days would have two mainframes, one to run the live systems, with the other being a backup machine that was normally used for development and testing."[13]

14. The GCHQ Witness gave a number of reasons why the likelihood of a contractor with system access rights going to the system, getting the relevant data and then covering their tracks, was low.

---

[10] Harold F. Tipton, CISSP. Micki Krause Nozaki CISSP. Information Security Management Handbook, 'Appreciating Organizational Behaviour and Institutions to Solidify Your Information Security Program' Sixth Edition, page 80

[11] Harold F. Tipton, CISSP. Micki Krause Nozaki CISSP. Information Security Management 'Appreciating Organizational Behaviour and Institutions to Solidify Your Information Security Program', Handbook, Sixth Edition, page 82

[12] Aeleen Frisch, O'Reilley & Associates Inc, Essential System Administration, December 1995, page 5.

[13] Ross Anderson, Security Engineering, 'A guide to building dependable distributed systems', Second Edition 2008, Page 323

15. I note that the risk is described as stated 'low' rather than it not being possible at all. A further concern is that senior members of staff appear unaware of this risk for several years because they did not know it was occurring.

16. The GCHQ witness goes on to address ways in which they seek to monitor and audit for malicious behaviour. The GCHQ Witness states that they do this at command line level but no information is given as to how this is carried out. The following explanation is given by the GCHQ witness:

> "21. Command line interfaces (an interface which relies on the user typing commands into the computer, rather than interacting with a user-friendly interface using mouse and keyboard as one would do for example with Microsoft Windows software) are used by the PU community to manage the system (e.g. installing software patches, monitoring performance, investigating problems). There is system monitoring and auditing for malicious behaviour at the command line."

17. If an admin has complete control over a system, then they can remove traces of their activity. An administrator with, according to GCHQ 14 "*full control*" or "*system admin*" or "*root*" accounts" can delete or modify an audit trail.

18. The GCHQ witness also states that "*Typically, within GCHQ the level of complexity of the systems means the only way to access to data in a readable format is via the software APIs where necessary and proportionality auditing is implemented.*"

19. I have consulted with my technical colleagues. This is a bad point. A privileged user can set up accounts (removing logging or oversight) on the software interfaces, alter the software packages run, or simply copy large volumes of data and convert it into meaningful information elsewhere. Further, the idea that a systems administrator cannot obtain access to very large volumes of comprehensible data is wrong. Mr Snowden is a straightforward example.

Statement of truth

I believe that the facts set out in this witness statement are true.

.....

Gus Hosein

20 December 2017