IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT 14/85/CH**

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT 14/120-126/CH**

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

Respondents

Expert report of Professor Ross Anderson

I, Ross John Anderson, will say as follows.

1. I am Professor of Security Engineering at Cambridge University where I have been a member of faculty at the Computer Laboratory since 1995. I am a Fellow of the Royal Society and the Royal Academy of Engineering, and have won the Lovelace Medal, the top UK award in computing. I am also an elected member of Council, the University's executive body.

2. I have worked or consulted for a wide range of technology companies both before joining Cambridge and since, including IBM, Microsoft, Intel, Google and Samsung. I have also consulted for financial services and utility firms from Standard Chartered Bank to the Electricity Supply Commission of South Africa. I have over thirty years' experience working with computer and communications security, including cryptography, in both industry and academia. My CV can be downloaded from my web page[1].

3. Since coming to Cambridge in 1992 I have made pioneering contributions to a number of new areas of research and practice, including the economics of information security, crypto protocols, API security, digital copyright marking and hardware tamper-resistance.

4. The grand challenge tackled by my research is developing the discipline of security engineering: building systems to remain dependable in the face of malice, error or mischance. This focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves. Security engineering is inherently multidisciplinary, as the hard problems in a globalised world usually have interlinked challenges in engineering, psychology, and economics.

5. This report is chiefly concerned with items 5 and 6 (d)-(f) in the Proposed Legal Issues and the consequences of seeking or inducing weaknesses in security facilities. By using computer and network exploitation (CNE) to obtain easier access to information, GCHQ and its partner agencies often inflict very substantial harm on others and indeed on the economy as a whole by weakening the essential electronic infrastructure upon which the world's economy and stability depends. This 'equities issue' is already recognised in US policy and a number of senior former intelligence community officials now acknowledge that the NSA and FBI got the balance wrong in the past[2]. UK policy and oversight need to be reconsidered accordingly.

[1] See http://www.ross-anderson.com or http://www.cl.cam.ac.uk/~rja14

[2] "Obama administration explored ways to bypass smartphone encryption", Andrea Peterson and

[2] "Obama administration explored ways to bypass smartphone encryption", Andrea Peterson and Ellen Nakashima, Washington Post, Sep 24, at https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html

Scope

6. Security engineering is not just about protecting 'computers' from hacking but about the large and growing number of systems that rely on computation, communication or both. Examples include card payment systems, prepayment electricity meters, burglar alarms, goods vehicle tachographs and speed limiters, taximeters and vending machines[3]. (I have been engaged in research and/or development work on all of these.) New systems coming onstream now or in the near future include implantable medical devices, remotely piloted aircraft and self-driving cars.

7. Every single one of these devices is of active or potential interest to law enforcement and intelligence agencies, and every single one uses cryptography, access control mechanisms, or both – the same mechanisms used to protect email and e-commerce against snoopers and hackers.

8. Thus when we talk about law-enforcement access to systems we are not merely discussing who can read your email. Who can read your electricity meter? (The drugs squad would like to know who's running a lot of lamps.) Who can defeat your burglar alarm? (Perhaps the covert-entry teams at MI5 would value that.) And can a police officer stop your car other than by stepping in front of you and raising his arm? (There are discussions on technical standards for doing just that with autonomous vehicles and indeed even for vehicles controlled by human drivers[4].)

9. Starting in the 1970s with the invention of the microprocessor, computers have been finding their way into more and more devices. In the 1990s these were called 'embedded systems'; in the 2000s 'things that think'; nowadays it's 'the Internet of Things'. More and more devices contain software, and communicate with online services.

10. Online communications can be a lifesaver. Many modern cars will alert a central reporting centre if the airbags deploy. Many have an emergency call button with which the driver can summon help after an accident. There is no need for people injured in a car crash to die slowly at the side of the road because no-one called 999 for an ambulance[5].

11. Even toy dolls now talk to data centres. Kids love toys that respond to their voices, but doing voice-recognition in the toy itself would cut the battery life to days or even hours. The solution is to send the child's speech over the home wifi to a remote data centre

[3] See my textbook "Security Engineering", RJ Anderson, Wiley 2008; also available free online at http://www.cl.cam.ac.uk/~rja14/book.html

[4] "EU has secret plan for police to 'remote stop' cars", Bruno Waterfield and Matthew Day, Daily Telegraph 29 Jan 2014

[5] "Lamara Bell dies of injuries sustained in M9 car crash", Libby Brooks, The Guardian, 12 July 2015

where it can be understood and commands send back to the toy[6]. Gesture interfaces are also spreading, and the video-recognition tasks involved are even more computationally intensive and thus even more likely to be done remotely.

12. A 2014 report by the US President's Council of Advisers on Science and Technology predicted that because of the spread of voice and gesture interfaces, almost every inhabited space on the planet will soon have in it microphones and cameras that are connected to data centres, many of them in everyday devices[7].

13. It will become increasingly common for the software in everyday devices, like the software in a PC or phone, to be updated remotely by the vendor or service provider. This enables businesses to add features and marketing offers. In the case of safety-critical products such as cars it will let some problems be fixed remotely, avoiding the cost of physical recalls, and making it feasible to fix more problems. It will also be ever more important to fix such security vulnerabilities as are discovered from time to time.

14. Thus when we discuss computer and network exploitation (CNE) for the purposes of intrusive surveillance we are not just talking about objects that are recognisably a 'computer'. Many other devices can also be pressed into service.

15. A law enforcement or intelligence agent wishing to place a crime boss under surveillance could also somehow access the microphone in his child's toy, or the server in the data centre that turns the speech into text and thus into commands to the toy.

16. A drugs gang that always deals heroin in the back of a moving taxi could be placed under surveillance by a traditional radio microphone, inserted physically under the seat; alternatively, agents could hack the dealer's mobile phone and turn on the microphone; and if the dealer leaves his phone at home, agents could hack the car and turn on the microphone used for voice commands, or even the microphone provided to make emergency calls.

17. Successive FBI chiefs have complained that the world is 'going dark' because of encryption[8]. The reality is that although some service providers turn on encryption (often to stop competitors stealing their ads), the spread of computers and communications has created a cornucopia of new sources for law enforcement and intelligence. It used to cost thousands of pounds a day to follow a suspect around; now, mobile phone location traces

[6] "Privacy advocates try to keep 'creepy,' 'eavesdropping' Hello Barbie from hitting shelves", Sarah Halzack, Washington Post, 11 March 2015

[7] "Report to the President – Big Data and Privacy: A Technological Perspective", President's Council of Advisers on Science and Technology, May 2014

[8] See for example Director James B. Coney at Brookings Institute, 16 October 2015; text at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

are easily available. And while people used to do business on the phone or in person, now people use email, text and chat. Material that would only be recorded if someone took the trouble is now archived automatically and is potentially available as evidence unless every single recipient takes the trouble to delete it, and does so competently.

The costs and risks of CNE

18. It is against this background that the Tribunal should consider the proper regulation of computer and network exploitation (CNE) for law enforcement and intelligence purposes. Where the 'Proposed Legal Issues' document refers to a 'device', it can mean not just a smartphone, but also you car, your electricity meter, your child's toy doll or even the laboratory equipment being used to analyse your blood test in a hospital. The same goes for the Home Office's Draft Equipment Interference Code of Practice.

19. I first consider the use of CNE by a law enforcement agency against a named individual target when they have a warrant to do so. The targeted surveillance of someone against whom an investigator has shown probable cause, or reasonable suspicion (depending on the jurisdiction), to an independent party who has assessed whether the intrusion is proportionate and necessary, is a reasonable extension of how civilised societies have dealt with law enforcement intrusion into physical property for many years.

20. Targeted CNE does however face several challenges. First, the intrusion may render any information collected difficult or impossible to use in evidence; the target, or some other criminal defendant, might claim that any evidence claimed to be found on his computer had been put there by the police. Whether such a claim is true or not in any particular cases, its possibility has consequences. My colleague Professor Peter Sommer, who has extensive experience in computer evidence, will discuss them in a separate report.

21. Second, the intrusion may place lives at risk. For example, in one of the first distributed denial-of-service attacks, an ISP (Panix in New York) had its service taken down by political opponents who hacked a number of servers in hospitals in Oregon and installed malware on them. These servers then bombarded Panix with traffic, depriving its customers of Internet service[9]. The hospital servers were easy targets because their FDA certification required them to be kept in an insecure state; they could not be upgraded with security patches as this would have voided their safety approval. Interference by hackers with medical equipment carries clear and present risks.

22. No harm to patients was reported in the Panix case, and while patients have been killed by software failures in a number of other reported cases, we do not yet have any documented incidents of people being killed by hacking attacks against machines on

[9] "Distributed Denial of Service Attacks", Charalampos Patrikakis, The Internet Protocol Journal Volume 7, Number 4

which they depended. (Hacking attacks have cost lives in other contexts; see for example the two suicides reported by the police in Canada following the Ashley Madison hack[10].)

23. Nonetheless, in my opinion it is only a matter of time before CNE causes fatal accidents. Computers are becoming embedded in ever more devices, on which human societies depend ever more in ways that are complex and ever harder to predict.

24. In addition to safety hazards, CNE carries political risks that have been underestimated in the past. A recent example if the disclosure that GCHQ hacked Belgacom in order to conduct surveillance of EU institutions[11]. Given that much of the UK's law is made there, this is almost as if the First Minister of Scotland had authorised Police Scotland to conduct surveillance of Whitehall by hacking BT. The Tribunal might ponder whether such an operation would have ever taken place if it had required specific authorisation, whether from a minister or a judge.

25. For this reason, security experts are overwhelmingly opposed to the use of CNE on a vigilante basis even in those jurisdictions where it is still legal. It is simply not safe to "hack back", as the machine that is being used to attack you and which you want taken offline might be providing a safety-critical service somewhere, or might belong to an institution with some kind or power or authority that could harm you.

26. Yet despite the hazards of hacking unknown devices, criminals routinely do so, mainly in order to assemble botnets – collections of compromised machines under their command and control which they use to perform criminal tasks, such as sending phishing emails (emails that purport to be from your bank and invite you to enter your bank credentials at a fake website) and mounting denial-of-service attacks.

27. We analysed the costs to the UK and global economy in a 2013 report commissioned by the Chief Scientific Adviser at the Ministry of Defence. While some specific cyber crimes can be costed separately, an ever-larger part of the direct cost of cybercrime relates to the shared infrastructure created to support crime – most notably the 'botnets' or networks of infected computers which criminals create in order to send spam, conduct phishing attacks against bank credentials, launch distributed denial-of-service attacks for hire or for ransom, and even host unlawful content. The global direct costs are estimated to be of the order of $4–5bn while the indirect costs – the time and effort taken to clean up infected machines – is estimated at $10bn for companies and the same again for individuals. The broader social costs to the global economy include a further $10bn to individuals of economic activity avoided because of fear of cybercrime, while the cost to merchants of people being reluctant to shop online because of security concerns is double

[10] "Toronto police report two suicides associated with Ashley Madison hack", Sam Thielman, The Guardian, 24 August 2015

[11] "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm", Der Spiegel, 20 September 2013

that again[12]. Because of the difficulties in measuring the costs of crime, these must be seen as no more than defensible order-of-magnitude estimates. However it is notable that an earlier Cabinet Office report estimated the direct and indirect costs of cybercrime to the UK economy at about double the figures in the 2013 report[13].

Use of CNE by nation states and their proxies

28. There have been many news stories of large-scale attacks on networks and computers that caused significant disruption, including attacks on civilian infrastructure in Estonia and Georgia after these countries had disputes with Russia. Thsee attacks were said by some to be the work of the Russian state but ascribed by others ethnic Russian hackers[14]. There were also some very damaging attacks on Sony that were said by the US government to be the work of North Korean state agents[15].

29. My own group has direct experience of an attack from China on the private office of the Dalai Lama in 2008 at the time of the Beijing Olympics. We received a call for help from the Tibetan government in exile and I sent an Indian research student, who happened to be in Delhi at the time, up to Dharamsala to help. We discovered that perhaps 35 of the 50 PCs in the Tibetan leader's office had been compromised and information was being sent to three locations in China associated with military and intelligence units tasked with different aspects of Tibet policy. For this and other reasons we were prepared to name the Chinese state as the likely responsible party. Chinese officials protested at this; their line was that criminals must have done it. Indeed, the software tools used to penetrate and then remotely control the Tibetans' machines were crimeware tools, freely available on the Internet, and used subsequently by Russian crime gangs. Further details can be found in our technical report, "The Snooping Dragon."[16]

30. The Snowden papers inform us that it is also NSA policy that where possible CNE operations should use crimeware tools against targets that might be competent at defending themselves, or be able to call on competent assistance. The main reason is deniability; a secondary reason is that an agency will not want to needlessly risk a

[12] "Measuring the Cost of Cybercrime", Ross Anderson Chris Barton, Rainer Boehme. Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage, The Economics of Information Security and Privacy, (Springer 2013) pp 265–300

[13] "The Cost of Cybercrime", Cabinet Office, 2011

[14] See for example "2007 cyberattacks on Estonia", Wikipedia

[15] "Obama imposes new sanctions against North Korea in response to Sony hack", Dan Roberts, The Guardian, 2nd January 2015

[16] "The Snooping Dragon – social-malware surveillance of the Tibetan movement," Computer Laboratory Tech Report TR-746, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.html

valuable asset, such as a vulnerability of which no-one else is aware and which can therefore be used to get covert access to high-value adversary systems.

31. The 5 eyes and other governments have been investing in CNE for intelligence, defence and law enforcement purposes at ever-greater scale in recent years. Since the 2010 publicity for the Stuxnet attack on Iran's uranium centrifuge facility at Natanz[17], the market prices for vulnerabilities have surged.

32. This has led to significant unease in the industry about 'vulnerabiity stockpiling'; that rather than reporting problems with the systems on which we depend, many agencies keep them secret, with a view to using them for offensive purposes.

The vulnerability ecosystem

33. Vulnerabilities can be thought of as the computer equivalent of loopholes in the law. As the law on some subject gets complicated, specialists notice interactions that the lawgiver did not foresee and which may (for example) enable a company to pay less tax. Eventually this is noticed, and once enough firms start using the loophole, the law is changed. In exactly the same way, the software that runs on a computer, phone, car or other device becomes more complex over time as new features are added; eventually, security researchers or others notice that sequences of instructions which the designers had not foreseen have some interesting effect, such as enabling unauthorised programs to be run on the device. If this is exploited at sufficient scale, then eventually the software will have to be changed. This may be expensive: cars may be recalled to a garage for patching, while railway signals may require a visit from a technician.

34. It is expensive to change software, just as it is expensive to change laws. Our society mitigates the cost of law change by leaving many of the rules in regulations that can be changed by statutory instrument, or in CPS or other guidelines that can be changed by order. Similarly, many steps have been taken to reduce the cost of changing software to fix vulnerabilities as they are discovered. Microsoft automatically ships a bundle of patches to Windows PCs every month, and the software of many but not all mobile phones is upgraded regularly.

35. There is also a software industry tradition of responsible disclosure, whereby security researchers or others who discover vulnerabilities report them to the software maintainer in confidence in advance of making them public. For example when our team discovers flaws that could affect banking systems we typically disclose them to regulators (the FCA, the US Federal Reserve, the European Central Bank) who in turn pass the news on to Visa and MasterCard who in turn inform equipment vendors and their member banks. This gives the vendors time to work out how to fix their systems and ship upgrades to their users. Public disclosure might follow 3–6 months after that, or longer depending on

[17] See for example "An unprecedented look at Stuxnet, the world's first digital weapon", Kim Zetter, Wired, 11 March 2014

the circumstances. This convention aligns incentives in that the researcher gets rewarded with publicity while the vendors are pushed to fix the flaw rather than hushing it up. In the case of vulnerabilities in common operating systems and network software, disclosure may be to the vendor, the maintainer, or a computer emergency response team (CERT).

36. This convention is backed up by further mechanisms. First, major systems and software firms such as Google, Apple and Facebook operate "bug bounty" programs, whereby security researchers who report vulnerabilities get paid directly. Second, there have been overt markets in vulnerabilities since about 2003 when iDefense and Tipping Point were set up. Their business model was to report the vulnerability to the vendor but meanwhile warn their own customers, who would enjoy additional protection in the time window between the vulnerability's being reported and its being finally fixed. This was one of the early industrial applications of the discipline of security economics that I helped found.

37. Since 2000, the 5 eyes powers have enjoyed privileged access to vulnerabilities reported to the CERT system. This was part of a deal that ended the "Crypto Wars", the struggle between the NSA and the tech industry over the regulation of cryptography, to which I will return later. At the time I was a consultant to Intel and under NDA; the NDA has now expired. The deal as it was reported to me was that the NSA would stop pushing to restrict the use of cryptography in ways that were harming US industry and instead rely on the exploitation of vulnerabilities that occurred naturally. The mechanism is as follows: when a vulnerability is reported to a CERT, it flows through the CERT network to the main CERT in Pittsburgh, which then reports it to the vendor. CERT also has staff with security clearances who also report it to the NSA. So the NSA has advance knowledge of vulnerabilities that have been reported but not yet fixed. (The UK government also set up a UK CERT under the aegis of the Security Service but this is nowhere near as centrally located as the US one, which receives information from CERT teams in thousands of organisations worldwide.)

38. This was how the world worked from about 2000–2010: thousands of vulnerabilities discovered by many people independently would flow to vendors to get fixed; or flow via CERT in which case the NSA, GCHQ and 5 eyes partners got a few months' exploitable advantage; or flow via vulnerability markets such as iDefense in which case their customers got a few months' advance protection instead. In either case, within a few months the fix would become available to all.

39. Things changed from about 2010 with the growth of a second generation of vulnerability markets consisting of companies whose customers did not want to get protection, but to do attacks. Companies such as Vupen and Hacking Team started selling to government agencies rather than to corporate America; they either sold hacking tools, that would enable a police force or intelligence agency to take over a suspect's laptop or mobile phone directly, or they sold vulnerabilities that the agencies could use in their own tools.

40. As a result, the amount of money available to a researcher who found an exploitable vulnerability in Windows or Android or iOS increased from perhaps $10,000 to over $100,000.

41. The trade in vulnerabilities can be understood by studying a large cache of emails leaked from Italian cyberweapons manufacturer Hacking Team, in July 2015[18]. These emails make their own business practices clear and also contain intelligence on their competitors. According to initial press analyses of the leak, Hacking Team were not just selling malware to NATO governments but to many repressive states, including Russia, the Sudan and Uzbekistan, something they had denied doing[19]. The Hacking Team leak followed a hack of a UK competitor, Gamma, in 2014[20]. These leaks confirmed that the 5 eyes agencies are major purchasers of vulnerabilities and of tools incorporating them.

Effects of CNE preparations on the wider software economy

42. These attempts by NSA, GCHQ and other governments' agencies to acquire and stockpile vulnerabilities have so increased demand as to cause real damage to the software ecosystem. For example, I learned in 2012 that a volunteer to the Webkit free software project, which develops and maintains graphics software for use in browsers, had been discovered trying to sneak a vulnerability into the software, with a view to selling it later. This sort of behaviour was profoundly shocking to the free software community; it might perhaps be compared to a news of a parliamentary draftsman accepting a bribe from a company to insert defective language into a Finance Act so as to create a loophole the company might exploit. While one might expect overt lobbying (e.g. of ministers), a disclosure of covert manipulation of the legislative machinery could significantly undermine trust.

43. Such behaviour had been unknown before it became possible to sell vulnerabilities for six-figure sums, and it poses a real problem for the industry. Much of the software on which we rely is built on free software platforms; FreeBSD is the basis for Apple's operating systems and Linux for Google's, while almost everyone's browser uses Webkit and most of the world's web servers run Apache. Some of this software is provided by companies who want others to use their standards, in order to get commercial advantage elsewhere (for example, Apache was originally written by a consortium of firms including IBM and Hewlett-Packard in order to provide a shared platform to compete with Microsoft). But much is written by volunteers, such as computer science graduate

[18] See for example "Hacking Team: A Zero-day Market Case Study", Vlad Tsirkeivich's blog, 22 July 2015

[19] "Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim", Alex Hern, The Guardian, 6 July 2015

[20] See for example "Top gov't spyware company hacked; Gamma's FinFisher Leaked", Violet Blue, ZDnet, 6 Aug 2014

students, who acquire both skills and reputation capital thereby, rather like law students interning as judges' clerks. It will impose very considerable costs on industry if all contributions to free software projects have to be vetted carefully for malice.

44. For this reason, industry views the stockpiling of vulnerabilities by the NSA, GCHQ and others with great alarm and, in the USA at least, has lobbied hard for a change in policy, particularly after the 2013 Snowden revelations make clear the scale of the program to facilitate CNE. This has now become a sensitive issue in Washington.

45. The industry feeling of violation was exacerbated by the Snowden revelation that GCHQ had been collecting Google traffic in transit between the company's data centres, in order to circumvent the encryption used by default on the links to users. Such network exploitation was seen as a gross breach of trust and left firms determined that law-enforcement access should only be through the front door, by due process of law.

46. The Snowden documents reveal that NSA / GCHQ built significant infrastructure to facilitate global CNE, with references to systems such as FOXACID (for launching malware against targets), TURBINE (to control a network of TURMOIL implants), and WARRIORPRIDE apparently a proxy network of infected machines providing 'scapegoat targets' through which exfiltrated material could be relayed. Technical information is fragmentary but taken together the disclosures suggest that large numbers of innocent people's computers were taken over and used for intelligence or law enforcement purposes without their knowledge or consent.

47. Following the Snowden revelations, President Obama set up a Review Group to advise him what to do about surveillance. The group consisted of three eminent lawyers (Cass Sunstein, Peter Swire and Geoffrey Stone), former counterterrorism tsar Dick Clarke, and former acting CIA Director Michael Morrell. It recommended inter alia that the NSA cease and desist from vulnerability stockpiling; that it should focus on its defensive mission rather than its offensive one, and see to it that vulnerabilities were patched as quickly as possible. President Obama implemented most of the Review Group's recommendations; in this case he did not agree unconditionally but rather ordered the NSA to set up a review process. A former NSA director admitted stockpiling in May 2014[21] but by November 2014 the administration was claiming that it now kept back only a very small number for offensive use, and reported the vast majority to vendors[22].

48. There are further costs that follow from the agencies undermining network and other security standards, for example by restrictions on encryption, and from their preparations and actions to target intermediate systems, from Internet routers to wifi hotspots. These

[21] "Former NSA chief defends stockpiling software flaws for spying", Andy Greenberg, Wired, 7 May 2014

[22] US Gov insists it doesn't stockpile zero-days to hack enemies", Kim Zetter, Wired, 17 November 2014

preparations form part of the same security/intelligence/law enforcement tool chain; compromised routers and weak encryption can be used to insert malicious payloads into the communications between endpoints of interest leading to one of them being compromised, even if the endpoints cannot be compromised directly. I will set out the background to encryption restrictions, and describe their effects; then deal with attacks on network infrastructure.

Restrictions on encryption

49. The Prime Minister recently indicated that he would like to see restrictions on encryption that would ensure it never got in the way of law enforcement and intelligence. President Obama is unconvinced but the Director of the FBI has publicly supported the Prime Ministers position.

50. In response to this, an international group of experts on cryptography, including myself, wrote a paper, "Keys under doormats" which explains in detail why this is a very bad idea. I include the paper as Appendix A. It has been published as an MIT technical report and accepted for the Journal of Cybersecurity.

51. Most of us were members of a previous expert group which in 1997 responded to an attempt by President Clinton to control cryptography with an earlier paper, "The risks and costs of key escrow"[23], which our paper in Appendix A brings up to date.

52. There had been a number of sporadic attempts in the 1970s and 1980s to restrict the civilian use of cryptography by using export controls, by steering research funding away from areas considered sensitive, and by giving key researchers consulting work so as to draw them within the security clearance system. Yet cryptography became steadily more important in key commercial applications including ATM and point-of-sale networks (where I first started working in the field), prepayment utility meters (where I was also a pioneer), software licensing and pay-per-view TV.

53. Cryptography is not just a tool for military and diplomatic communications confidentiality. It provides dependable mechanisms for linking your bank PIN with your account number; for generating the magic code needed to credit your electricity meter; and for ensuring that your software will work, or your set-top box will decipher the football, so long as you pay your subscription. It has become a general-purpose mechanism for taking trust from where it already exists to where it is needed. My expert group colleague and co-author Ron Rivest describes it as being "duct tape". It's what we use to bind digital objects together.

54. The agencies had seen cryptography as their "turf" and now had to watch as it escaped to become a mainstream commercial technology. And control was slowly being lost: the

[23] H Abelson, RJ Anderson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption", World Wide Web Journal v 2 no 3 (Summer 1997) pp 241–257

agencies had managed to see to it that the Data Encryption Standard, widely used by banks, had a rather short key, and banks realising this started to use multiple encryption. The ever-widening applications of cryptography caused more and more engineers to learn about it and to start contributing innovations.

55. Business for its part became increasingly resentful at the inconvenience and insecurity caused by export controls on cryptographic technology. For example, in 1989 I was working for a large bank in Hong Kong and discovered that the ATM networking there used encryption that was completely insecure. Smart criminals who had wiretapped the ATM network could have deciphered all the passing PINs, recorded the associated account numbers, and forged cards on an industrial scale, possibly forcing the ATM network to be closed. It had been felt impossible to get properly certified hardware encryption devices not just for the network switch but for the 46 member banks; despite the fact that Hong Kong was a British colony at the time, a number of the banks were controlled from mainland China. Eventually the big banks decided to upgrade the cryptography and push hard for the necessary export licenses. At that time, we were suffering substantial credit card fraud by Chinese gangs in the region and needed to introduce CVVs (the 3-digit security codes on card mag strips and signature strips), which are also generated and verified by the hardware encryption devices. Multiple annoyances such as this were creating steady pressure for governments to liberalise cryptography.

56. In 1993, however, the Clinton administration announced the Escrowed Encryption Standard, or Clipper chip. The offer was that firms who switched to this standard would be able to export devices containing cryptography. The catch was that the chip contained an NSA master key, and the design supposedly had the property that encrypted material could be decrypted by the intended recipient, and also if need be by the NSA.

57. In short order, a cryptographer at Bell Labs (Matt Blaze, one of my coauthors on the two crypto policy papers) found a flaw in this design[24], and the Clipper chip was abandoned.

58. Several further attempts were made by the US, UK and other governments to come up with technical proposals for controlling commercial cryptography. GCHQ sponsored the development of a key-management protocol for public-sector use, which was showed by a number of academics to have flaws, just like Clipper[25]. There was a proposal that all cryptographic keys should be put in "escrow" with a "trusted third party"; so all key services would have to be licensed, and a licensing condition would be that the service operator kept copies of the key to hand to GCHQ. The European Commission objected because keys are also used for electronic signature, and third parties with spare copies of

[24] "Protocol Failure in the Escrowed Encryption Standard" MA Blaze, Proceedings of the 2nd ACM Conference on Computer and Communications Security: 59–67

[25] "The GCHQ Protocol and its Problems" RJ Anderson, MJ Roe, Eurocrypt 97 pp 134–148

keys could forge signatures. Industry objected that government demands to control cryptography were hindering innovation and harming public confidence in e-commerce.

59. While this debate was raging, the UK and US governments prevented the export of cryptography using keys longer than 40 bits. Such keys are weak as they can be found by trying all 2^{40} (about one trillion) possibilities. Longer keys required licenses, so could not be used in mass-market equipment. Licenses were granted only for specific applications such as banking and often only after lengthy and opaque negotiations about the capability of the equipment concerned. This hindered innovation and led directly to serious harm.

60. For example, the content scrambling system used in DVD disks had to use 40-bit keys and as a result was easily broken. This meant that video copyrights could be infringed by illicit copying, and that the region control coding scheme used by the film industry to release new videos at different times in different parts of the world was defeated. This in turn meant that studios had to pay for worldwide marketing of films from the day of release rather than test-marketing them in the USA first.

61. Another example comes from WEP, the first system used to encrypt wifi. Its vulnerability meant that people could get service without paying, and that supposedly secure wifi networks could be penetrated in order to attack devices using them. The most high-profile resulting loss was claimed to have been the theft of over 40 million customers' credit and debit card details from TJ Maxx, millions of which were sold to fraudsters[26]. The hacker Albert Gonzales was arrested with $1.65m in cash and got 20 years. The costs to affected companies, including banks who had to reissue compromised cards, were reported in hundreds of millions.

62. Some industries were permitted to use slightly longer but still inadequate keys. For example, the most common contactless smartcard system for many years was the Philips Mifare, variants of which have been used in many systems from the Oyster Card to the door locks on the building where I work. The Mifare card used 48-bit keys and was broken ten years ago. As a result, the Oyster card could be cloned from October 2008 and TfL had to improve back-end systems to detect cloned card use[27].

63. Most of the remote key entry systems used in cars have been broken as they use defective cryptography designed in this era; a significant proportion of the theft of high-value motor vehicles in the UK can be traced, directly or indirectly, to the Crypto Wars. Many other vulnerable systems are still in service, forcing system operators to implement system changes or mitigations at great expense, or live with the risk of breakins.

[26] "T.J.Maxx Data Theft Likely Due to Wireless 'Wardriving'", Larry Greenmaier, Information Week 9 May 2007

[27] "Why being open about security makes us all safer in the long run", B Schneier, The Guardian, 7 August 2008

64. Another victim of weak keys is the authentication in CANBUS, the standard way for components in a car to talk to each other. An attacker who can run malicious code in a car radio (for example) can progressively take over one vehicle component after another, until ultimately they have the engine control unit, the brakes, the accelerator and even the door locks. In 2010, researchers from UCSD and the university of Washington showed they could take over all but the steering wheel of a target vehicle[28]. This led others to experiment with hacking motor vehicles remotely, and recently to the recall of 1.4 million vehicles by Chrysler after hackers showed they could take over 2014 and 2015 model Jeep Cherokees over the Internet[29].

65. Where products supported weak keys for export but strong keys for domestic use in the USA or in 5 eyes countries, the key management mechanisms typically turned out to be vulnerable to attack.

66. One example is SSL/TLS, the protocol used to encrypt traffic to and from websites. Since its introduction two decades ago. this has suffered repeated “downgrade” or “rollback” attacks where an attacker tricks the communicating parties into believing that the other party is using export-grade cryptography. Most recently, the FREAK attack[30] targeted export-grade RSA keys, and embarrassingly the vulnerable websites included whitehouse.gov and nsa.gov (in total, over a third of websites were vulnerable including large commercial sites such as American Express and Groupon).

67. Another is the BBK (Barkan-Biham-Keller) attack on GSM, the standard used by mobile phones for authenticating handsets and encrypting both speech and text messages. Again, there was a ‘strong’ algorithm A5/1 and an ‘export’ version A5/2[31]. It turned out that an attacker who listens to a conversation encrypted with the former can then replay the authentication protocol later to the handset, asking it to use the latter. The handset generates the same encryption key it used before, and this key can now be solved, enabling the earlier traffic to be read. This vulnerability persists to this day despite the later introduction of an ‘even stronger algorithm’ A5/3. The result is that foreign intelligence services who maintain sigint facilities in their embassies in London can decipher the mobile phone calls and texts of high-value UK targets.

[28] Experimental security analysis of a modern automobile, Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, IEEE Symposium on Security and Privacy 2010

[29] “Fiat Chrysler recalls 1.4m vehicles in wake of Jeep hacking revelation”, The Guardian, 24 July 2015

[30] CVE-2015-0204

[31] Instant ciphertext-only cryptanalysis of GDM encrypted communications, E Barkan, E Biham, N Keller, Journal of Cryptology v 21 (2008) 392–329

68. Another is the hugely complex design of IPSEC, the protocol used in most virtual private networks (VPNs) on which many companies rely to protect confidential data in transit across public networks. This resulted from the NSA/GCHQ demand to have an export version that does authentication only. Snowden revelations about all VPNs being breakable, and about collection of IPSEC key negotiation traffic worldwide, have since undermined firms' confidence in VPN products.

69. A current topic is BGPSEC. At present, the networks that collaborate to form the Internet trust each others' route announcements, which are not strongly authenticated. Problems can occur when one network announces that it has good routes to certain IP addresses and this causes other networks to send it traffic for those addresses, where this is not appropriate. For example, Pakistan Telecom tried on 24th February 2008 to censor YouTube by announcing that it had good routes to YouTube; this announcement was visible worldwide rather than just in Pakistan, leading to 2 hours and 15 minutes of global service denial. In another incident, China Telecom announced on 8th April 2010 that it had good routes to many US and other addresses, causing about 15% of the world's Internet traffic to flow via China for 18 minutes. Some people thought this was backscatter from a Chinese test of a "cybernuke"; my own view was that it was probably an honest mistake[32]. Nonetheless it's clear that malicious route announcements could do grave damage to the Internet's routing infrastructure, and in consequence a suite for authentication protocols for interdomain routing, BGPSEC, is currently under standardisation. However BGPSEC doesn't stop route leaks or relay attacks, and some people are concerned that the GCHQ/NSA input to this process is having an effect similar to that on X.509 and IPSEC. To put it bluntly, perhaps the agencies are more concerned with their ability to take out the Internet in hostile countries in times of tension than they are with preventing hostile actors (including terrorists) doing the same to us.

70. The laws and regulations enacted to impose export controls on cryptography also inflict collateral damage. In the 1990s the US pushed the UK to extend export controls from tangible items such as tanks and planes to intangibles such as software. The result was the Export Control Act 2002. This was opposed by research scientists, including then President of the Royal Society Lord May, as it brought under the export control regime not just cryptographic software but software written by academics to control many types of scientific equipment that were subject to export licensing. The effect is that perhaps tens of thousands of academics, as well as tens of thousands of software developers, are technically breaking a law of which most are completely unaware. Those of us who are aware of the law can circumvent it with ease (by putting software in the public domain by making it available on our websites).

[32] For a discussion of these incidents and BGP security generally, see"Resilience of the Internet Interconnection Ecosystem", Panagiotis Trimintzios, Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzouios, ENISA, 2011

Indirect costs of GCHQ / NSA controls on commercial information security

71. The persistent attempts by GCHQ and its 5 eyes colleagues to see to it that commercial information security is only just ‘good enough’ impose serious costs indirectly. For example, during 1995–6 I advised the BMA on the safety and privacy of medical information systems, and one of the issues was whether medical records, test results and so on could be sent by email. After we suggested that personal health information be protected using available free software tools such as PGP, the Department of Health commissioned a report from a consultancy that took advice from GCHQ and recommended a government-use system with key escrow. GCHQ saw this as a means of marketing their key escrow agenda but the technology was inappropriate. First, there is no need for government access to keys when at least one endpoint is always an NHS organisation and the government thus has access to the plaintext anyway. Second, the use of a closed proprietary system cut sharply the number of possible competing suppliers.

72. The end result was first that the NHS initially adopted an obsolete email standard (X.400) which delayed the adoption of proper email in the NHS by several years; second, that BT became a monopoly provider of NHS networking, with the result that the DSL link to a GP practice costs perhaps ten times as much as a similar link supplied by the same company to a vet next door; and third, that for some years the focus of information security in the NHS was keeping out ‘hackers’ rather than preventing abuse of authorised access by insiders, which is by far the main source of abuse. In short, a misguided GCHQ policy led to NHS networking being late, expensive and insecure.

73. As a second example, I worked on standards for authenticating communications in electricity substations with a student who was sponsored by ABB to work on this problem. The US government had realised that its electricity transmission and distribution infrastructure might become vulnerable to cyber-attack and had pushed the regulators and standards bodies to come up with solutions. Consultants were hired and a proposal, which became draft IEC 62351, according to which communications between devices in a substation would be digitally signed. This was however not implementable as some of the messages between meters, controllers and switchgear must be delivered within 5ms, and the cryptographic processors capable of executing the specified digital signature algorithm quickly enough are subject to US and UK export controls. The standard had to be redesigned to focus on protecting communications from the substation to the network control centre using such mechanisms, while traffic on the substation’s local area network would be protected either physically or using message authentication codes that can be computed and verified quickly in software. This whole debacle held up for several years the standards process and thus the prospect of protecting power grids, both in the USA and here, from cyber-attack using standard cryptographic mechanisms.

Deliberately weakening systems to facilitate LE access

74. In addition to the weaknesses in encryption algorithms and protocols described in the section above, there have been sustained and harmful efforts to modify system designs in

other ways to facilitate law enforcement and intelligence access. This is partly done by overt means such as CALEA (the US Communications Assistance to Law Enforcement Act, which enables the US authorities to order the suppliers of communications hardware and software to build in wiretap facilities), and partly by covert deals, of which the most notorious was the backdoored elliptic curve random number generator.

75. In that case, the 'Dual_EC PRNG' was designed by the NSA and standardised by NIST. It was used to generate cryptographic keys. It is now believed that the NSA, knowing secret parameters, can predict the random numbers it generates and thus the keys. As the generator is slower than need be, adoption incentives were needed, and it is reported that the NSA paid RSA Data Security, the main supplier of encryption toolkits to developers, $10m to embed it by default in its product. The contract between RSADSI and the NSA was among the Snowden leaks. The collateral damage has included the credibility of NIST as a cryptographic standards-setting body; NIST had to abandon proposed changes to the cryptographic hash function SHA-3 as the crypto community is no longer prepared to trust it.

76. It is not only the US government that pushes telecommunications equipment providers to insert wiretap facilities; GCHQ has been doing the same since at least the early 1970s when standards were set for the first electronic telephone exchanges. It cooperates with other agencies in Europe to standardise mechanisms via ETRI. In addition to providing interfaces of signals intelligence agencies to collect traffic, under various warrantry regimes, from the operator with its cooperation, such mechanisms are sometimes also exploited covertly, and academic researchers have criticised the quality of security protection engineered around these back doors. In a famous case, law-enforcement access features standardised by ETRI in GSM base station and back-end systems were exploited to hack Greek government mobile phones in 2004 during the Athens Olympics. A team of unknown attackers subverted the wiretap facilities in the network of Vodafone Greece to tap the mobile phones of the Prime Minister, the Minister of Defence and other prominent Greek officials[33].

77. Yet another example of subverting commercial computer-security products was revealed again in the Snowden papers with the story that GCHQ / NSA had been reverse engineering and finding ways to subvert anti-virus software[34]. The news that security software can also be a vector of infection by state actors can have a chilling effect on normal users' willingness and ability to protect themselves. The cynical may ask whether it's significant that the antivirus firm in the story is a Russian one, which disclosed the existence of Stuxnet. Is this GCHQ / NSA's revenge? Are Western antivirus firms like Symantec and McAfee trusted not to find US / UK government malware? I have no answer to these questions, but once people start thinking in these terms, trust in the whole

[33] The Athens Affair, Vassilis Prevelakis and Diomidis Spinellis, IEEE Spectrum 29 June 2007

[34] "GCHQ and NSA broke antivirus software so that they could spy on people, leaks indicate", Andrew Griffin, 23 June 2015

industry is undermined. It becomes more difficult to get people and firms to take even rational action to mitigate real threats from cybercriminals and hostile state actors.

Conclusion

78. In conclusion, GCHQ has been engaged at all material times with the NSA and its other 5 eyes allies in a sustained, directed and generously funded programme to facilitate CNE by restricting the use of strong information security mechanisms such as cryptography, undermining their effectiveness by subverting the design and implementation of cryptographic protocols, random number generators and other essential system components; compelling the introduction of backdoors into infrastructure and other products by manipulating technical standards or as a condition of export licensing; positioning itself in the vulnerability reporting ecosystem so as to take covert advantage of naturally-occurring vulnerabilities reported in good faith for remediation; and subverting the market for vulnerabilities by bidding up the price of exploits that are not thereafter reported to vendors for closure.

79. This had imposed very substantial costs on industry and society as a whole. It has facilitated common criminality such as car theft. It has undermined the confidence of prospective customers overseas in the trustworthiness of security and other products offered by UK suppliers. It has damaged public confidence in the trustworthiness of online services, which imposes direct costs on industry; bank customers are more expensive to service in branches than online, and the same goes for much of the retail sector. In general the indirect costs of security breaches are significantly larger than the direct costs.

80. The equities issue is now discussed openly and frequently in the serious business press, not just the technical community. For example, The Economist writes on Sep 13 2015: *"Digital weapons have their drawbacks. Iran's nuclear programme was delayed, not derailed. But they present problems for America's military planners. They involve discovering and exploiting weaknesses which potentially affect everyone, not just America's enemies. The NSA, post-Snowden, is under fire for having deliberately weakened commercial cryptography to ease its espionage efforts. A digital weapon that sabotages power stations could also be discovered and used by America's foes."* As a result, industry has pushed back hard.

81. I would like finally to refer the Tribunal to a report in the Washington Post, "Obama faces growing momentum to support widespread encryption", Sep 16 2015, and a leaked National Security Council document discussed therein "Review of Strategic Approaches". The document and the story suggest very strongly that the US Government is moving towards abandoning the policy of pushing for back-door access to systems and instead favouring defence over attack. This is also a position that many eminent former members of the US national security establishment have adopted as the relative costs have become clear. These are not just economic costs but also relate to the West's soft power – our ability to be a beacon for democracy and human rights in a troubled world

must also be balanced against the minor additional gains that might flow to intel and law enforcement if the rules online were to be less onerous that the rules offline.

82. I refer in particular to the statements of former NSA Director Mike McConnell and former Homeland Secretary Michael Chertoff to the effect that despite the legitimate concerns of law enforcement about encryption, "the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."

83. They continue, "The administration and Congress rejected the Clipper Chip based on the reaction from business and the public. In addition, restrictions were relaxed on the export of encryption technology. But the sky did not fall, and we did not go dark and deaf. Law enforcement and intelligence officials simply had to face a new future. As witnesses to that new future, we can attest that our security agencies were able to protect national security interests to an even greater extent in the '90s and into the new century."

84. The overriding public interest is in protecting the security of the digital infrastructure on which we are all increasingly coming to rely. The actions of GCHQ / NSA have caused, and will continue to cause, damage to that infrastructure and to our computer and communications security more broadly by systematically interfering with security and cryptography – via standards, via export controls, and now via the large-scale deployment of CNE.

85. The US administration thankfully seems to be realising that this was a strategic mistake.

86. I am happy to provide the Tribunal with further information, if so requested, and to appear before it.

Signed

Ross John Anderson

Cambridge, September 30th 2015

Appendix A: "Keys under doormats", MIT CSAIL-TR-2015-026, July 2015