LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's response to the Home Office consultation on the Equipment Interference Code of Practice

March 2015

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

Bella Sankey
Director of Policy
Direct Line 020 7378 5254
Email: bellas@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sara Ogilvie
Policy Officer
Direct Line 020 7378 3654
Email: sarao@liberty-human-rights.org.uk

Introduction

1. On 6 February 2015, the Home Office published a consultation on a draft Equipment Interference Code of Practice (the 'Draft Code) pursuant to section 71 of the *Regulation of Investigatory Powers Act 2000* (RIPA). On the same day the Investigatory Powers Tribunal ('IPT') published its second judgment in the action brought by *Liberty, Privacy International etc.*[1] The judgment held that the intelligence-sharing relationship between the UK and US was unlawful prior to December 2014, because rules governing the UK's access to the NSA's mass electronic surveillance programmes PRISM and Upstream were secret and therefore breached Articles 8 or 10 of the European Convention on Human Rights (ECHR). In December 2014, the Tribunal held that GCHQ's access to NSA intelligence was lawful from that time onward because secret policies governing the UK-US relationship were made public during the case. Liberty disagrees that the limited safeguards revealed are sufficient to make GCHQ's mass surveillance and intelligence-sharing activities lawful, and will challenge the Tribunal's December decision at the European Court of Human Rights.

2. The Draft Code is the first Code of Practice on equipment interference (commonly known as 'hacking') to be published despite RIPA being in force for almost 15 years. The timing hints that the Draft Code responds to two further cases already lodged in the IPT concerning disclosures about UK and US Government equipment interference practices made by former NSA contractor, Edward Snowden. These cases have been lodged by Privacy International (PI) and a collective of internet and communications services[2]. By putting more information on its equipment interference activities in the public domain, it appears the Government hopes to prevent further adverse judgments from the IPT. It is noteworthy and disappointing that the present consultation takes place not against a background of voluntary increased transparency on the part of Government but in the context of piecemeal action in response to litigation. Notwithstanding this, Liberty is pleased to have the opportunity to respond to the present consultation.

[1] Liberty (the National Council of Civil Liberties) & Others v Secretary of State for Foreign & Commonwealth Affairs & Others, 6 February 2015, Case Nos: IPT/13/77H, IPT 13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH.

[2] Greennet Limited, RiseUp Networks Inc, Mango Email Service, Korean Progressive Network, Greenhost, Media Jumpstart Inc and Chaos Computer Club.

Equipment Interference

3. Equipment interference – also known as Computer Network Exploitation ('CNE') – is an incredibly intrusive new form of surveillance. It enables the State to conduct the most comprehensive form of surveillance on an individual that has ever been undertaken and also has the potential to compromise and destroy the security of individual devices and networks affected as well as the entire internet.

4. The Draft Code states that it applies to *"(i) any interference (whether remotely or otherwise) by the Intelligence Services or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions and (ii) information derived from any such interference…".*[3] Information includes content and communications data as defined in section 21 of RIPA. The Draft Code lists how the Intelligence Services may apply CNE capabilities: to obtain information from and about equipment; to locate, examine, remove, modify or substitute hardware or software to yield such information; and to enable and facilitate surveillance activity by means of the equipment.[4]

5. The Draft Code does not explain the technical capabilities involved in CNE but Liberty has benefited from sight of PI and Open Rights Group's submission to the present consultation which contains a detailed explanation of the technology underlying CNE and in particular (1) what equipment may be targeted, (2) what information can be obtained, (3) how it is obtained and (4) what harm may result. PI and ORG explain that the *"type of equipment that can be targeted is vast, ranging from personal computers, and mobile phones to wifi-enabled televisions, smart meters and energy grids, and communications network infrastructure…Additionally, any device that is connected to a modern network…such devices now include televisions, refrigerators, baby monitors, smart meters, smart Barbies and a myriad of others".*[5] The information that can be obtained is described in the following manner:

> *"The intelligence agent can access any stored data, including documents, emails, diaries, contacts, photographs, internet messaging chat logs, and location records on mobile equipment. He can see anything typed into the device, including login details and passwords, internet browsing histories and draft*

[3] Paragraph 1.6 of the Draft Code.
[4] Chapter 10 of the Draft Code.
[5] PI and ORG Submission in response to the consultation on the Draft Equipment Interference Code of Practice.

documents and communications the user never intended to share. He can recover files that have been deleted. He can control any functionality, including surreptitiously turning on the microphone, webcam and GPS-based locator technology. He can even re-write the code that controls the device, adding new capabilities and erasing any trace of his intrusion. And he can overcome any attempts by the user to protect her privacy, not only by accessing information that was never meant to be shared, but also by overcoming encryption and secure communications methods."[6]

6. PI and ORG describe the various methods used for CNE, including the most common methods for deploying malicious software ('malware') via "social engineering" "watering hole" and "man in the middle" attacks.[7] These techniques include sending emails impersonating individuals or organisations with which the target is familiar; infecting all visitors to a particular website; and interrupting and tricking two parties who think they are having a direct conversation into having two separate conversations with the hacker. As regards the latter technique, a leaked GCHQ document sets out their analysis that "man in the middle" attacks cannot currently be lawfully authorised in the UK.

7. In addition to CNE's intrusive impact on individuals and their devices, its potential to undermine device, network and internet security is cannot be overstated. PI and ORG describe how "*the security hole created can be exploited by anyone with the relevant technical expertise*"[8] including those furthering a criminal purpose. Some of the methods that can be used for CNE (for example the use fake links that may be forwarded on or posted in public forums) mean that the user may have no control over the spread and impact of their hack. Similarly, attacks on network administrators create the infrastructure for mass surveillance of their subscribers. The potential for a hacker to create, delete or alter content undetected, creates a chilling capacity for evidence-tampering and miscarriages of justice. The long-term security implications of CNE operations make it a unique form of highly sophisticated surveillance that carries unlimited and untested potential for Government to act against the security and economic interests of its own citizens, whether advertently or otherwise.

[6] Ibid.
[7] Ibid.
[8] Ibid.

Current Practice

8. Liberty understands that the UK Intelligence Services have been engaged in CNE for over a decade. The Snowden files reveal a plethora of programmes:

a. CAPTIVATEAUDIENCE is used to take over a targeted computer's microphone and record conversations taking place near the device.
b. GUMFISH covertly takes over a computer's webcam and takes photographs.
c. FOGGYBOTTOM records logs of internet browsing histories, collecting login details and passwords for email accounts.
d. SALVAGERABBIT copies data from removable flash drives that connect to an infected computer.
e. Disclosed documents also reveal that GCHQ has developed extensive means of manipulating mobile devices – in particular iPhone and Android devices. Since 2010 these tools have allowed for: the activation of a microphone and the taking of recordings without the user's consent; precise identification of the geographical whereabouts of the user; retrieval of any content from the phone; and the avoidance of detection that the device has been compromised.

9. Further leaked documents, listing a range of tools and techniques developed and employed by GCHQ, advise GCHQ employees that *"If you don't see it here, it doesn't mean we can't build it."* The capabilities and descriptors listed on that page include the capacity to:

a. change the outcome of online polls (UNDERPASS),

b. inflate the views on a webpage (SLIPSTREAM),

c. spoof any email address and send email under that identity (CHANGELING),

d. clone websites and undertake "on the fly" alterations (HAVOK),

e. "masquerade" wall posts on Facebook for "individuals or entire countries" (CLEAN SWEEP).

While a number of these tactics can be used to facilitate and trigger the industrial-scale deployment of malware onto devices, they also raise serious questions about the manner in which hacking can be used to manipulate and distort reality in a way

that goes far beyond the use of hacking for the purpose of surveillance and the collection of information.

10. Leaked documents also make clear that these invasive hacking techniques are being used not only against intelligence targets but also against innocent individuals and key global infrastructure networks to enable mass surveillance. OPERATION SOCIALIST combined both of these approaches. According to analysis of the Snowden files by The Intercept news site, the computer systems of a Belgian telecommunications provider were infected by GCHQ with malware which allowed GCHQ to access private communications passing over the Belgacom network. To do this, GCHQ targeted individual engineers working for Belgacom and infected their electronic devices, resulting in the engineers going to a fake website masquerading as the Linked-in website which attacked the engineers' computers. This technique, known as QUANTUM, allowed GCHQ to have control of the computers and access the Belgacom networks. As reported by the Intercept website, this industrial hack went undetected for two years. An undated document notes in relation to quantum technique that *"GCHQ involvement may be in jeopardy due to British legal/policy restrictions."* The documents also contain the claim that GCHQ was close to accessing the central routers of Belgacom, with the next step being to deploy an even more aggressive "man in the middle" technique to attack smart phone users who have encrypted their communications.

11. The Intelligence Services have also reportedly leveraged these techniques to hack and attack "millions" of devices. According to documents, the NSA's automated processes to facilitate hacking were put into practice at GCHQ's Menworth Hill site. This allows the deployment of hacking and attack techniques without the need for human involvement and therefore further permits the use of hacking on a massive scale.

The Current Legal Framework

12. Hacking is prima facie unlawful as a matter of domestic criminal law. Section 1 of the *Computer Misuse Act 1990* makes it an offence to cause a computer to perform any function with intent to secure access to any program or data held within it if the access is unauthorised. Section 3 of the 1990 Act also makes it an offence to do any authorised act in relation to a computer if the intention is to impair its operation, hinder or prevent access to any program or data, to impair the operation of

any program or reliability of data. Section 10 provides that section 1 has effect without prejudice to the operation of any enactment relating to the powers of inspection, search or seizure, but this carve out does not apply to section 3.

13. There is currently no clear or accessible legal regime governing the hacking of property and devices by the Intelligence Services. Following the publication of the present draft Code of Practice, it is clear that the Government relies on enabling powers contained in sections 5 and 7 of the *Intelligence Services Act 1994* (ISA). Section 5 covers activity in the UK and provides that a warrant authorised and issued by the Secretary of State may make lawful any "*entry on or interference with property or with wireless telegraphy*". Applications for section 5 ISA warrants can be made by any of the Intelligence Services. The Secretary of State must believe that the warrants are necessary and proportionate for the purpose of assisting the requesting Agency with carrying out any of its functions, which are laid out in exceptionally broad terms in a number of statutes.[9] The recent ISC report sheds some further light on current practice. While the number of section 5 warrants obtained by the Agencies in 2013 is not disclosed, the report reveals that while the majority of warrants are targeted, a percentage were 'thematic' permitting the Agencies to use the same technique on multiple occasions or authorised 'IT Operations'.

14. Section 7 ISA covers operations outside the UK. It allows the Secretary of State to sign an authorisation that removes civil and criminal liability for activity which may otherwise be lawful under UK law. Section 7 authorisations last up to six months and can be renewed. The ISC report confirms that GCHQ and SIS obtain "class-based" authorisations under section 7 ISA enabling them to undertake *classes of activities* overseas that might otherwise be unlawful. SIS currently has eight class-based authorisations in place. They do not need to seek separate authorisation for any individual operation under these eight classes of activity, however they claim to seek additional ministerial authorisation where an operation might be particularly contentious or involve use of a new capability. Ministers are not otherwise kept informed of activity that takes place under class-based authorisations. The ISC reports that by October 2014, GCHQ had five section 7 class-based authorisations in place but the number of individual operations undertaken by GCHQ is not

[9] Section 1 of the Security Service Act 1989; Section 1 of the Intelligence Services Act 1994.

disclosed.[10] The only oversight currently provided is ex post facto, by the Intelligence Services Commissioner, who can review the class authorisations on a six monthly basis to satisfy himself that the statutory requirements have been met.

15. The Draft Code is divided into nine chapters. It restates the overlapping legal provisions which govern hacking and provides some further guidance on the use of section 5 ISA powers. The Draft Code strictly relates only to section 5 warrants as there is no power for the Secretary of State to issue Codes of Practice in respect of section 7 of the ISA. However paragraph 1.4 notes that "as a matter of policy" SIS and GCHQ must comply with the provisions of the Code in any case where equipment interference is authorised under section 7.

Human rights analysis

16. CNE capabilities carry the potential for even greater intrusion than the lawful use of any other single form of surveillance currently undertaken including interception, the deployment of covert human intelligence sources and directed and intrusive surveillance under RIPA, the execution of search warrants or the combined use of these other powers. As discussed above, CNE also opens the door to activity which goes far beyond State surveillance. CNE therefore engages several rights contained in the ECHR as incorporated into domestic law by the HRA. Article 8 (right to respect for private and family life), Article 10 (freedom of expression), Article 11 (freedom of association), Article 1 of the First Protocol (right to peaceful enjoyment of possessions), Article 6 (right to a fair trial), Article 14 (non-discrimination). Given the potential damage to computer security and corresponding vulnerability to criminal elements that results from CNE, the use of this technology arguably engages many more rights, including the positive obligations on the State to take steps to uphold Article 2 (right to life) and Article 3 (prohibition on torture and inhuman and degrading treatment). By section 1 of the HRA it is unlawful for a public authority to act in a manner which is incompatible with a Convention right. Each of the Intelligence Services is a public authority and therefore governed by this requirement.

17. While many of these rights are qualified and can be justifiably interfered with in pursuance of a legitimate aim, several – including the right to a fair trial and the prohibition on torture and inhuman and degrading treatment – are absolute. It is

[10] The Intelligence and Security Committee, *'Privacy and Security: A modern and transparent legal framework',* 12 March 2015.

noteworthy that by engaging in CNE, the Government will encourage a market for its use and further development to the potential detriment of us all. For all these reasons, Liberty would have expected State use of CNE to be subjected to the most robust public and parliamentary debate and if sanctioned, detailed and comprehensive regulation via primary legislation. The Government's current approach – to effectively legislate for CNE via a Code of Practice - is deeply undemocratic and contrary to our constitutional and Rule of Law traditions.

18. In the remaining section of our response we analyse the substantive shortcomings of the Draft Code and suggest the bare minimum of statutory protections required for State authorisation of CNE -

a. **CNE powers should be brought forward in primary legislation for full and detailed consideration by Parliament.** Given the capacity for CNE to be even more intrusive than powers governed by RIPA, primary legislation is urgently required.

b. **CNE is so intrusive it should be authorised only in the most serious and narrowly defined circumstances for example with regard to specific threats to life or limb or national security.** CNE should not be authorised to provide general operational capability nor to conduct speculative intelligence fishing expeditions. Liberty is deeply concerned that hacking can currently be authorised for the purpose of any of the broad functions of the Intelligence Services. SIS is, for example, mandated to obtain and provide "*information relating to the actions or intentions of persons outside the British Isles…in the interests of the economic well-being of the UK".*[11] This raises acute concerns –supported by the Snowden leaks - that hacking is considered to be justified in order to gain commercial advantage over other countries. The Draft Code provides no comfort that hacking is not being utilised in an expansive manner.

c. **CNE should only be authorised for targeted operations concerning specific individuals who, or devices which, are suspected of holding evidence relating to the most serious criminality.** By contrast paragraph 4.6 of the Draft Code states that a section 5 warrant only need provide "*the details of any offence suspected or committed where relevant*". This is deeply problematic and confirms the disturbingly speculative use of capabilities. The

[11] Intelligence Services Act 1994, section 1.

Code further contends that hacking activity may be conducted against people who are not intelligence targets in their own right and that such intrusion should not be considered "collateral intrusion" but rather "intended intrusion". Liberty accepts that the device of someone who is not an intelligence target may, in limited circumstances, be targeted. However the devices of those against whom there is no suspicion should be targeted only if there are objective and solid grounds to believe that the device itself holds evidence of the most serious forms of criminality. Absent this suspicion, it is wholly disproportionate to target the device of an innocent individual. **Additionally, "intended intrusion" must not be capable of justifying mass CNE surveillance via the targeting of network administrators.**

d. **The power to authorise CNE should not lie with the Secretary of State nor senior officials: instead CNE should be subject to the highest level of judicial authorisation.** Liberty is deeply concerned that, at present, the Secretary of State is responsible for authorising hacking operations. Of further concern are the relevant statutes and Draft Code which provide that a senior official may authorise a hacking warrant following discussion with the Secretary of State in cases where the Secretary of State is not available to give the authorisation. Liberty finds it deeply troubling that warrantry for the most intrusive type of surveillance is currently deputised to a senior civil servant. This state of affairs is, however, inevitable given that the responsibility for authorisation of section 5 and 7 warrants is restricted to two Secretaries of State. Liberty has written extensively about the need for prior judicial warrantry for all forms of RIPA surveillance in order for the Rule of Law to be upheld. The same arguments apply here with even greater force given the intrusiveness of CNE. In *Klass v Germany* the European Court of Human Rights made clear that, in an area where abuse is easy in individual cases and abuses have such harmful consequences for democratic society as a whole, it is desirable to entrust supervisory control to a judge:

> *"The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at*

least in the last resort, judicial control offering the best guarantees of independence, impartiality and proper procedure".[12]

David Bickford, former Undersecretary of State and Legal Director of MI5 and MI6 has recently said

"in my view…the extent of covert surveillance today and the pressures involved in its authorisation, particularly on the balances of necessity and proportionality, instruct us that the principle in Klass of judicial authorisation must now be applied."[13]

e. **Proportionality requires that CNE is only authorised in circumstances where all less intrusive capabilities (including interception), have been either tried or considered and rejected as being unable to provide the vital information sought.** Instead paragraph 2.6 of the Code provides that the proportionality test is whether the information sought could "*reasonably be obtained by other less intrusive means.*" It further provides that "*any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms*". The use of CNE for "operational or capability" reasons does not qualify as a legitimate aim for the justifiable restriction of qualified rights under the ECHR. CNE should only ever be authorised for pressing investigative reasons in the manner described at paragraph b above.

f. **CNE should not be deployed to enable mass surveillance.** The Code states that an application for a section 5 warrant should take account of the risk of obtaining information about persons who are not the subject of the warrant; described as "collateral intrusion." The Code further provides that measures should be taken to avoid or minimise this privacy intrusion. Liberty accepts that in the execution of certain surveillance techniques, some degree of collateral intrusion may be necessary and proportionate in certain circumstances. However, mass intrusion resulting in the surveillance of

[12] *Klass and others v Federal Republic of Germany*, European Court of Human Rights, 2 EHRR 214, 6 September 1978
[13] David Bickford CB, European Parliament Libe Enquiry, Judicial Scrutiny of Intelligence Agencies, 7 November 2013.

hundreds of thousands, millions or billions of communications cannot be properly classed as necessary "collateral intrusion" and is by its nature disproportionate.

g. **Warrants should be granted for a short duration in recognition of the seriousness of the intrusion of CNE.** Liberty is deeply concerned by paragraph 4.10 of the Draft Code which states that a warrant, unless renewed, lasts for six months. This is double the duration that some interception warrants may last. Paragraph 2.13 states that "*regular reviews*" of CNE warrants should take place to assess the continuing need for the warrant and the frequency of reviews should be determined by the applicant for warrant unless specified by Secretary of State. Reviews should be conducted as frequently as is considered necessary and practicable. These supposed safeguards are badly deficient for obvious reasons. the frequency of reviews should be prescribed and not left to applicants to determine.

h. **Comprehensive records must be kept on all authorised warrants and operations.** Liberty is pleased to note that paragraph 5.1 requires that centrally retrievable information on all section 5 warrants - including the result of periodic reviews - should be retained for at least three years. This requirement will presumably apply "as a matter of policy" to section 7 warrants and seemingly conflicts with current SIS practice. The ISC report discloses that SIS do not hold statistics about the number of operations involving entry or interference with property overseas and claim that "*to record this would be disproportionate*".[14]

i. **There should be a strong statutory presumption against CNE operations that risk accessing legally privileged and other confidential information that should only be rebutted in the most compelling circumstances.** The Draft Code largely replicates recently disclosed internal Intelligence Services policies on the interception of legally privileged and confidential information. The policies are woefully inadequate and dangerously undermine the integrity of our civil and criminal justice system. Liberty has commented further on the

[14] ISC report, paragraph 178.

shortcomings of these policies in our response to the consultation on the revised Interception of Communications Code of Practice.[15]

j. **Information obtained through hacking should be subject to strict statutory controls and only ever retained or disseminated in tightly defined circumstances in pursuance of investigations and prosecutions relating to serious criminality.** The Draft Code requires internal arrangements are in place for each of the Agencies to ensure that *"the disclosures, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services' functions…"* Breaches of the arrangements are to be reported to the Intelligence Services Commissioner. The *"number of persons"* and *"extent of disclosure" are to be "limited to the minimum necessary".* This applies to persons within an Intelligence Service and outside. It is enforced by *"prohibiting disclosure to persons who do not hold the required security clearance, and also by the need to know principle: information obtained by equipment interference must not be disclosed to any person unless that person's duties are such that he needs to know about the information to carry out those duties."* These obligations further apply to anyone to whom the data is subsequently disclosed: *"in some cases this may be achieved by requiring the latter to obtain the originator's permission before disclosing the information further".* The same obligations apply to the copying of the data. By paragraph 6.10, information obtained via hacking *"must be marked for deletion and securely destroyed as soon as they are no longer needed for the functions or purposes [of the Intelligence Services]".* These controls – while more detailed than the guidance in place for disclosure of information gathered via interception – fall woefully short. By sanctioning retention and further dissemination of information by reference to the Intelligence Services functions, the guidance creates a set of circular and perfunctory safeguards.

k. **There should be an absolute prohibition on creating, altering or deleting content on a device accessed via a CNE operation.** Paragraph 6.3 of the Draft Code makes clear that *"information obtained through equipment*

[15] Liberty's response to the Home Office consultation on the Interception of Communications Code of Practice, paragraphs 17-22.

interference may be used as evidence in criminal proceedings".[16] Liberty supports the use of information obtained via lawful surveillance in criminal proceedings. Indeed, one of the principal justifications for State surveillance should be the pursuance of prosecutions for serious crime. However CNE capabilities allow the Intelligence Services complete control over devices allowing an agent to delete, alter or create stored content or communications while leaving no trace of their actions. There should therefore be a cast-iron prohibition on such activity and an obligation to record, in a verifiable manner, all action taken in relation to a device so that disclosure can be provided in respect of evidence relied upon in criminal proceedings. Liberty is deeply alarmed at the lack of safeguards in place to guard against data tampering and implications for the integrity of the UK's criminal and civil justice systems.

l. **The extension of CNE powers to non-Agency individuals should not be permitted.** Liberty is troubled that the Draft Code twice states that section 5 and section 7 warrants can be sought in respect of "*members of the Intelligence Services, or persons acting on their behalf or in their support*". This is a significant extension of CNE – and other unfettered powers - with far-reaching ramifications. Sophisticated CNE operations should only ever be authorised in respect of serving members of the Intelligence Services.

m. **Those whose devices are hacked should be notified of this once the operation has been concluded unless there are clear grounds for maintaining secrecy.** Liberty supports post-surveillance notification for all forms of State surveillance. If a person's human rights may have been breached, in order to have access to an effective remedy, the person must first be made aware of a possible breach. This was confirmed by the European Court of Human Rights in *Klass v Germany* in 1978 and reiterated in *Weber and Saravia v Germany* in 2006:

> *The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in*

[16] It is noteworthy that this is in stark contrast to the present position in relation to data obtained through interception capabilities. As regards interception, the Government argues against admissibility on the grounds that it will require disclosure of sensitive capabilities and undermine security*:* it is unclear on what basis the Government draws a distinction between the impact of admissibility for both types of surveillance product.

principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see Klass and Others, cited above, pp. 26-27, § 57).[17]

We believe that once either an investigation has been completed or a suspect is no longer under suspicion he or she should be notified of the surveillance they have been subjected to unless there is a specific reason for maintaining secrecy. **Post-surveillance notification is even more important in the context of hacking due to the way in which the continuing security of a device is fatally compromised when a hack takes place.**

n. **The system of "classed- based" warrants and internal approval for individual operations should be ended.** Section 7(4)(a) of the 1994 Act provides that the Secretary of State may give an authorisation which relates to "*acts of a description specified in the authorisation*" The Draft Code confirms that a section 7 authorisation "*may be specific to a particular operation or user, or may relate to a broader class of operations*". The Draft Code provides that for individual operations under a class based authorisation, "internal approval" to conduct operations must be sought from a "designated senior official". An application for internal approval should contain the same information as an application for a section 5 warrant. Where particular individual operations under a classed-based warrant may result in the acquisition of confidential information, authorisation must be sought from an "Annex A approving officer". For any particularly sensitive operations the designated senior official or Annex A approving officer must consult the FCO or seek the endorsement of the Secretary of State. **This is the most enabling and permissive regime imaginable and imposes no credible restraint on the authorisation of CNE operations. Warrants for this highly intrusive form of surveillance should instead be required to be highly prescriptive in nature and relate to particular operations. Operations should not be internally authorised but rather independently authorised by a senior judge.** SIS argue that they need class based authorisations because seeking individual authorisations would "*place a significant and disproportionate bureaucratic burden on both SIS operational*

[17] *Weber and Saravia v Germany*, 2006, application 54934/2000, paragraph 135.

teams and the Foreign Secretary and FCO officials".[18] Given the intrusions at stake, the "disproportionate bureaucratic burden" argument does not suffice.

o. **Further urgent review and reform of section 7 ISA**. The consultation on the Draft Code has brought into focus the breath-taking power contained in section 7 ISA. While the consultation concerns the use of section 7 to authorise hacking, it is silent on the other types of activity authorised under the power. As the ISC noted in their report "*in recent years, many people have expressed suspicion as to the true nature of Section 7 of the ISA, with some referring to it as the 'James Bond clause' and suggesting that it might allow serious crimes to be committed".*[19] In the absence of further clarity or explanation on the activities authorised under section 7, this statement by the parliamentary body charged with oversight of the Agencies is chilling. Liberty believes that this enabling power which seemingly removes all manner of civil or criminal liability for authorised activity must be urgently reviewed and reformed. Instead of a catch-all exemption from liability for wrongdoing, the Agencies powers should be explicitly set out in detailed and prescriptive primary legislation.

[18] ICS report, paragraph 237.
[19] ISC report, paragraph 236.