LEGAL CHALLENGE TO UK INTERNET SURVEILLANCE

Briefing Note

Facts

Since the first disclosure of documents regarding the US National Security Agency (NSA)'s collection of US phone records from on 5 June 2013[1] the British public has witnessed a series of alarming disclosures regarding the extent of the surveillance programmes operated by US and UK intelligence services[2]. The source for the vast majority of these reports has been leaks by the whistleblower Edward Snowden. The extent of internet surveillance by the UK government is far greater than the public, experts and even Members of Parliament had previously thought. The disclosures have sent shock waves around the world. Two programmes in particular have been at the centre of the revelations:

1. **PRISM** – an operation by the NSA which enables it to gather a wide range of internet communication content (such as emails, chat, video, social network posts etc.) and metadata (technical identificatory data) from the major US internet corporations. The UK Government has been able to tap-in to this resource and obtain information of persons of interests even where interception warrants have to be obtained in respect of such individuals for interception by UK authorities.[3]

2. **TEMPORA** – a UK Government programme for tapping, storing and analysing all electronic data passing into or out of the UK through the undersea fibre-optic cables that route data between Europe and America. The programme is carried out by Government Communications Headquarters (GCHQ). A similar programme in the US named **UPSTREAM** has also been exposed.

The disclosures show that the vast majority of our internet communications are being seized, stored and searched by the UK and US Governments. EU citizens living outside the UK are also directly affected, not least because many of their internet communications will be routed via America through the UK.

Legal Challenge

Big Brother Watch[4], Open Rights Group[5] and English PEN[6], together with German internet 'hacktivist' and academic Constanze Kurz[7] have launched a legal challenge to the UK's internet surveillance activities before the European Court of Human Rights. They argue that such unchecked surveillance is a breach of theirs, and our, Right to Privacy under Article 8 of the European Convention on Human Rights. Any interference with that right must be proportionate and in accordance with adequate and published legal standards. The law and practice in the UK fails to meet either requirement.

---

[1] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[2] http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html
[3] http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[4] http://www.bigbrotherwatch.org.uk/
[5] http://www.openrightsgroup.org/
[6] http://www.englishpen.org/
[7] http://inka.htw-berlin.de/inka/constanze/

The Applicants initially sought to bring their case in the UK domestic courts and wrote to the UK Government on 3 July 2013 stating that a judicial review challenge would be brought. However the Government told the Applicants that they would have to make a complaint to the Investigatory Powers Tribunal (a tribunal that hears complaints against the intelligence services in secret). The European Court of Human Rights has held in the case *of Kennedy v UK* that it does not require applicants to complain to the Investigatory Powers Tribunal before making an application to Strasbourg, due to concerns about its effectiveness and its power to grant the remedy that they seek. The Applicants have therefore issued proceedings in the European Court of Human Rights, which will determine whether UK law breaches international law. It is believed to be the first international law challenge based on the Snowden disclosures.

UK internet surveillance is predominantly regulated by the Regulation of Investigatory Powers Act ("RIPA")[8]. This is supposed to ensure that internet surveillance is the exception, not the rule. But it has failed. Because many of our internet activities can be deemed "external" to the UK, the Government is able to certify that they are tapped, stored and analysed by GCHQ (under section 8(4) RIPA). External communications are those where a sender or recipient is outside the UK, as will very often be the case. These 'global' warrants issued for the TEMPORA programme appear to be granted on a continual 'rolling' basis. Furthermore, the information extracted appears to be freely available to intelligence partners such as the NSA. It is equivalent to having all the letters passing through the UK intercepted, stored, copied and capable of being read by a potentially unlimited number of intelligence agencies around the world, where this is regarded as being in the "interests of national security".

At the time RIPA was enacted it was not even clear to legislators whether or not internet communications would be capable of being intercepted in a useful way. Certainly there was no public awareness of the enormous implications of the powers granted by RIPA to the intelligence services.

Similarly, GCHQ's use of PRISM data to spy on our internet activities has also gone unchecked. Regulators in this country appear to have been entirely unaware of it until the public disclosures. The most important of those regulators, the Parliamentary Intelligence and Security Committee, quickly looked into the matter and issued a clean bill of health within weeks of the revelations[9]. But further examination shows that investigation to have been extremely narrow in its scope and the two page report hardly scratches the surface[10]. This entire area is entirely unregulated by any law or published regulations.

Remedy

The Applicants are asking the Court to declare that the UK's internet surveillance practices are disproportionate and that the legislation intended to protect the public's rights to privacy in this context is not fit for purpose. The practice of issuing surveillance warrants has failed and/or been circumvented and those responsible for oversight have failed.

[8] http://www.legislation.gov.uk/ukpga/2000/23/contents
[9] http://isc.independent.gov.uk/
[10] http://www.theguardian.com/world/2013/jul/17/prism-nsa-gchq-review-framework-surveillance

The Applicants ask the Court to order the UK to adopt internet surveillance practices that recognise our rights to privacy. This means new laws that require surveillance to be proportionate; to be overseen by judicial authorities acting in public; that permit notification of persons affected by surveillance (even if after the fact); that are overseen by adequately resourced and empowered regulators. In short, a legal regime that recognises the Principles on the Application of Human Rights to Communications Surveillance.[11]

The Applicants are fundraising for their legal costs. See https://www.privacynotprism.org.uk/).

[11] https://en.necessaryandproportionate.org/text