**Civil Society Concerns about UK Surveillance**

Secret mass surveillance is a threat to democracy and the rule of law. If we are unable to know about the extent of government surveillance, we are unable to protect our fundamental rights. The revelations, made possible by the whistleblower Edward Snowden, over the past few months have shown without doubt that Parliament has been kept in the dark about the powers and capabilities of GCHQ to conduct mass surveillance.

We believe the  points below are core to the debate surrounding oversight of the UK's intelligence and security services:

**1. All of our communications are caught up under GCHQ spying.**

GCHQ is conducting indiscriminate, dragnet surveillance by intercepting fibre-optic cables carrying global communications that pass through the UK, via the Tempora programme. The content of internet and telephone communications passing across roughly one quarter of the "wavelengths" carried by international fibre optic cables that land in the UK is analysed, with content recorded for three days, and records kept for thirty days.  Internet users in the UK will have their communications intercepted as they interact with global service providers; as will international users of UK internet service providers.

The GCHQ project has, since 2008, steadily been building capability and now claims to provide the “biggest internet access” of any intelligence agency in the Five Eyes alliance of eavesdropping agencies (US, UK, Canada, Australia, New Zealand) . In 2011 “more than 39bn events in a 24-hour period” were recorded producing “larger amounts of metadata collection than the NSA".

GCHQ's senior legal advisers describes the UK as having “a light oversight regime compared with the US". This is all made possible through a 'certificated warrant' signed by the Secretary of State, in the interest of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom. These warrants are re-authorised every six months by the Secretary of State. Limited oversight comes from the review of warrants by the Intelligence and Security Committee, the Interception of Communications Commissioner, and the Investigatory Powers Tribunal – [ http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf ]
 There is no before-the-fact judicial control of interception, and since intercepted material cannot be introduced into court proceedings, no meaningful judicial review either.

While former GCHQ director Sir David Omand continues to insist "the government is not going through all your personal emails because it's a computer doing it rather than a person", the European Court of Human Rights has found[amann1] that interception and storage of a communication constitutes a privacy violation, and that the “subsequent use of the stored information has no bearing on that finding“[amann2] nor does it matter “whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way“[amann3]. Simply put, they agree that there is a scale of intrusion, but reject the idea that there is *no* intrusion in automated collection/analysis of data.

**2. Mass Surveillance is wrong and unlawful.**

Any act of surveillance by a state that violates the right to privacy must be in accordance

with the law; be proportionate and be necessary in a democratic society. Mass surveillance can never be regarded as in accordance with human rights law  given the serious risk it poses, not only to the right to privacy but to the fundamental nature of the democratic state and of human dignity. As the UN Special Rapporteur on freedom of expression has noted, “mass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance.”[specialrap] Mass surveillance places everyone under the spectre of being watched, thereby chilling our free expression and promoting conformity. The broad purposes of the surveillance and its secret nature prevents open debate and deliberation in Parliament, thereby preventing democratic authorisation and oversight. "If you have nothing to fear, you have nothing to hide" is not the language of a democratic society. Our right to privacy forms the bedrock upon which all of our other rights and freedoms are built. The Lords Constitutional Committee (2009) agreed that "Mass surveillance has the potential to erode privacy. As privacy is an essential pre-requisite to the exercise of individual freedom, its erosion weakens the constitutional foundations on which democracy and good governance have traditionally been based in this country."

It is clear that mass surveillance is the antithesis of British values.

**3. This policy has already been rejected twice**

In 2008 the previous Government proposed the creation of a centralised database of communications data to be stored by GCHQ. After a consultation this policy was abandoned. When the government next proposed the policy in 2009, GCHQ's centralised database was omitted and there was widespread (cross party?) agreement about the risks of such an approach. In 2012 when the draft Communications Data Bill was introduced, the Government was clear that it was not seeking to establish a centralised database [see William Hague, http://www.theyworkforyou.com/debate/?id=2012-06-20a.863.1 and Nick Clegg http://www.telegraph.co.uk/technology/technology-video/9180886/Nick-Clegg-totally-opposed-to-central-e-mail-and-phone-call-database.html] It is clear that when debated in public and in a democratic manner, valid concerns are aired, discussed and addressed.

It now transpires that much of what was hoped to be achieved as part of the draft Communications Data Bill was already being done, in secret, by GCHQ in the form of their Tempora programme. The role of the British Parliament, and the wishes of the British public, were ignored and dismissed out of hand.

Parliament has been told that Ministers approved surveillance, and that approval is the basis for legality. We’ve seen in the US, a disagreement between what the President believes he had authorised, and what their intelligence agencies believed had been authorised.

- What did UK Ministers believe they were approving?
- What were UK Ministers briefed on?
- What were GCHQ operational staff told about what Ministers had approved?

**4. Hurts the UK's standing in the world**

British law and policy sets the standard for many countries around the world. The deployment of mass surveillance capabilities without democratic authorisation sets a terrible precedent that will likely be replicated unless Parliament acts to rein in these powers. Allowing GCHQ to operate with near impunity harms global human rights and

damages confidence in the internet economy as users across the globe decide to avoid British service providers and internet companies. We have already seen a financial cost to these programs. It was reported that the US cloud computing industry could lose up to $35 billion (£22.5 billion) over the next 3 years as a result of companies moving away from US providers due to fears relating to the PRISM program. [http://www.techweekeurope.co.uk/news/exposure-of-nsa-spying-programmes-could-damage-the-us-cloud-industry-124419] The UK cannot afford a similar reaction from the global business community.

For decades Britain has provided a strong voice defending liberty, democracy and respect for privacy against regimes that used mass surveillance against their own people. Therefore not only does mass surveillance create a real danger to the position of the UK as a global leader in modern technology, business, and trade, but more fundamentally it poses a risk to the export of British values across the world. Now Robert Mugabe's Zimbabwe is declaring that new laws requiring telecommunications firms to record and keep details of all phone calls, emails and text messages for up to 5 years, do not at all infringe on their citizens right to privacy. Zanu-PF's Deputy Director of Information said: "There's nothing amiss about that. It happens all over the world. Ask Edward Snowden.... This is a national security issue". [http://mg.co.za/article/2013-10-11-00-bob-can-listen-to-your-phone-call/] The UK is running this risk of being used a beacon for legitimising mass surveillance by repressive regimes across the world.

**5. Oversight only fixes part of the problem**

Oversight is only effective when it is conducted by a truly independent body that is subject to public scrutiny. Of course, a balance must be struck when dealing with national security, however the Intelligence and Security Committee falls short in this regard. It is instead being lauded by GCHQ for always being "exceptionally good at understanding the need to keep our work secret".[1] While the recent announcement that it will hold an Open Evidence Session on 7 November is to be welcomed as a step in the right direction, it will not cover ongoing programmes such as Tempora and the role of the agencies in mass surveillance. These issues are clearly deemed too sensitive for wider democratic debate. The neutrality and legitimacy of the role of the Committee in holding the agencies to account can only be  further undermined by the chilling effects of mass surveillance, and the knowledge that the programs exist and operate freely in the UK. Oversight must therefore be combined with transparency that can lead to informed public debate -- a debate that cannot help but conclude, for the reasons set forth above, that mass surveillance can never be proportionate in a democratic society.

[specialrap] (A/HRC/23/40), at [62].
[amman1] Amann v Switzerland (2000) application 27798/95; Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48
[amman2] Amann v Switzerland (2000) application 27798/95 para 69
[amman3] Amann v Switzerland (2000) application 27798/95 para 70