**Speaker Notes: Nick Pickles, Director, Big Brother Watch**

Good afternoon. Thank you for the invitation to speak to your committee today, as part of an enquiry that has an exceptionally important role in the current climate.

The internet has transformed our lives, our economy and is now arguably as essential a utility as water or electricity.

The explosion in smartphone use, the falling cost of computers, tablets and high-speed internet access have combined to revolutionise communications more in a decade than in the century that preceded it. The world is smaller – bringing our friends and our enemies closer to home. The internet is a global platform for commerce, for social interaction and for unprecedented surveillance.

May I begin by saying that the objective of Big Brother Watch, and of our litigation in the European Court of Human Rights, is not to bring about the end of surveillance. Our objective is to ensure that, as a democratic state, the United Kingdom's surveillance regime is fit for a digital age, with a legal framework that citizens can both understand and have confidence in.

I would also note an important feature of this debate that I feel has not been afforded proper attention, and in the past week in Britain has been accepted by a concerning proportion of our media. Namely, the idea that the internet is beyond surveillance, and that the ability of the states to monitor digital communications was only known to a limited few. This is patently absurd.

Edward Snowden has not exposed the fact that the internet is subject to surveillance. If that in itself is a crime then the makers of the Bourne films, the BBC's Spooks, the producers of Zero Dark Thirty and countless authors and writers are guilty of the same enemy aiding that Mr Snowden has been accused of.

What Edward Snowden has done is illustrate two key things. Firstly, that the scale and nature of surveillance is far beyond what has ever been publicly acknowledged or legislated for, whether the en masse collection of content through the Tempora programme or the work through Bullrun to undermine the encryption that proects our bank accounts, personal details and online transactions. Secondly, that where surveillance powers have been granted, they have been exploited with regard to the internet to a degree that few would recognise as features of a civil society and oversight mechanisms have proved woefully ill equipped to perform their tasks.

As Nigel Inkster, former deputy chief of MI6, told the Guardian: "I sense that those most interested in the activities of the NSA and GCHQ have not been told very much they didn't know already or could have inferred."

Edward Snowden has performed a great public service and I hope initiated a debate that will not remain confined to these hearings. Indeed, perhaps the starkest demonstration of how the scale of surveillance exceeded the intent of legislators is the current efforts of Representative Jim Sensenbrenner, a Wisconsin Republican and co-author of the Patriot Act, to significantly reduce the data being collected under the legislation he authored, on the grounds that the legal authority has been taken far beyond what Congress intended.

The response of the US Government, from the President down, to reform the law, enhance oversight and improve transparency demonstrates the very real public interest in these disclosures. It also highlights how the legal and ovesight frameworks are not fit for purpose.

It is a great shame that a debate on the same level is not taking place in Britain. However, I would also like to note that, contrary to any perception that the British public is not concerned by these revelations, our initial appeal to cover some of the costs of our legal action saw our initial target of £20,000 exceeded within a few days, an overwhelming public response.

Our legal action should be seen within this context. Debate may be denied by some, but it is not a debate that the public wish to ignore. Quite the opposite.

The UK's arrangements, with regard to the PRISM programme, were examined by the Intelligence and Security Committee in a report published in July 2013. In it, the ISC recognised that there is a question as to whether "*the current statutory framework … remains adequate*". It drew attention to the fact that in some areas the legislation was "*expressed in general terms and more detailed policies and procedures*" have had to be put in place (above §50-52). These concerns, although grossly understated, represent an implicit acknowledgement of the absence of applicable safeguards in the governing statutory regimes.

The committee did not consider the Tempora programme, perhaps because it had not become public knowledge, or perhaps they were not aware of the programme. Whichever may be true, Tempora that is a critical element of our legal action.

As Professor Korff noted this morning, there are serious concerns that GCHQ's activities are not properly regulated or overseen. The requirement than any infringement on Article 8 be prescribed by law, necessary and proportionate is well understood, however the UK's compliance with these tests is clearly of concern.

This is the central argument of the legal challenge that Big Brother Watch, along with fellow British NGOs the Open Rights Group and English Pen and Constanze was announced on Thursday 3 October.

We 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 said an action in the English Courts was barred and that the we should complain to the Investigatory Powers Tribunal, the secretive body that hears complaints about the intelligence agencies and

from which there is no appeal to the courts. However, proceedings before the tribunal would not permit the public examination of these important issues, nor are they capable of providing the remedy the applicants seek: a new legislative framework respectful of British and European citizens' privacy rights.

The European Court has previously held that the IPT does not provide an effective remedy and that it will hear complaints directly. The applicants have therefore pursued their legal challenge in the European Court of Human Rights. We believe that this is the first complaint to be made to an international court relating to the disclosures of the Prism and Tempora programmes.

We remain ill informed of the legal basis of the Tempora programme. This is a failure of legislation, oversight and transparency.

Let me turn to the basis of this legal action.

In *Kennedy v United Kingdom* (2011) 52 EHRR 4 at [93], the European Court of Human Rights recognised that the evident risk of arbitrariness in a secret power to intercept communications rendered it "essential" to have clear, detailed rules on interception, especially as the technology available for doing so is becoming continually more sophisticated. It observed at [94] that it would be contrary to the rule of law for the legal discretion granted for interception to be expressed in terms of an unfettered power. It also observed (at [160]) that "*indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of the Regulation of Investigatory Powers Act 2000*" ("**RIPA**"). The Court has also held that Article 8 jurisprudence must adapt to technological developments in *Weber v Germany* (2008) 46 EHRR SE5 at [93], and observed that in the context of rapidly developing telecommunications technology, legislative frameworks governing the safeguarding of private information and electronic correspondence must be "*particularly precise*" (*Uzun v Germany* (2012) 54 EHRR 121 at [61]).

Simply, in our case we submit technologies have now been developed, and have for some time been in use, which *do* permit the indiscriminate capture of vast quantities of communication data, which can then be passed between States, and which is not subject to any sufficiently precise or ascertainable legal framework and is beyond effective legal scrutiny.

We contend that the reported activities of GCHQ constitute a violation of Article 8 of the ECH. In relation to receipt of foreign intercept material—i.e. the receipt, use, retention and dissemination of information received by UKIS from foreign intelligence partners which have themselves obtained it by communications intercept—the legal framework is inadequate to comply with the "*in accordance with the law*" requirement under Article 8(2).

In relation to GCHQ's own generic interception capability, the provisions contained in RIPA relating to external communications warrants allow UKIS to obtain general warrants permitting indiscriminate capturing of vast amounts of communication. As such, our claim argues that there is no legislation (or other legal provisions) in the UK that can be said to "*give citizens an adequate*

*indication of the conditions and circumstances in which the authorities are empowered to resort"* to the measures referred to (*Uzun v Germany* (2012) 54 EHRR 121).

We submit British legal provisions do not enable persons to foresee the general circumstances in which external communications may be the subject of surveillance (other than that any use may be made of communications if considered in the interests of national security—a concept of very broad scope in UK law); they do not require authorisations to be granted in relation to specific categories of persons or premises; they permit indiscriminate capture of communications data by reference only to its means of transmission; and they impose no significant restrictions on the access that foreign intelligence partners may have to such intercepted material. In short, there are no defined limits on the scope of discretion conferred on the competent authorities or the manner of its exercise. Moreover, there is no adequate degree of independent or democratic oversight. Indiscriminate and generic interception and the legal provisions under which it is carried out thereby breach the requirements that interferences with Article 8 must be "*in accordance with the law*" and must be proportionate.

This generic GCHQ intercept of external communications merely on the basis of the happenstance that they have been transmitted by transatlantic fibre-optic cables is an inherently disproportionate interference with the private lives of the thousands - perhaps millions - of people whose private data has been intercepted and examined by the UKIS for no better reason than its means of transmission.

In effect, the power to obtain and use external communications data by means of intercept is unfettered in published law, as long as it is thought broadly to be in the interests of nation security or other of the specified generic purpose. There are no adequate criteria by which a court or tribunal could assess the legality of use of any particular intercept material even if the courts had jurisdiction to do so, which they do not.

As Ian Brown states in his expert testimony for our case, within the current legal framework *"It is possible therefore that a typical warrant authorising the Tempora*
*programme may be as wide as "'all traffic passing along a specified cable running between the UK and the US".*

*In the light of the Guardian's revelations, the performance of the UK oversight bodies*
*and officials has clearly been deficient. It is difficult for members of the public to have*
*confidence that their privacy is being adequately protected by a system that operates*
*with such little transparency. A global surveillance system of breathtaking scope has*
*been built with no public debate, authorised under sweeping secret warrants from the*

*Secretary of State, with opportunities only for classified discussion and scrutiny incamera by the Intelligence and Security Committee, The system of internal GCHQ rules for human rights compliance is similarly designed and operated in secret, with nowhere near the level of detail of scrutiny published by the Interception of Communications Commissioner to command public confidence.*

Contrast this with the situation in the US, as outlined by Cindy Cohn in her testimony as part of our ECHR filing.

*On 21 August 2013, the DNI declassified two FISA court rulings confirming the existence of both §702 programmes, and explaining problems with the UPSTREAM programme.26 Notably for these purposes, the problems arose from the retention and searching of United States persons' information. The bulk seizure, collection, search and analysis of the communications and communications records of non-United States persons was not questioned or limited by these decisions.*

The absence of legal safeguards is particularly concerning in the context of the receipt of data such as that obtained under the PRISM and UPSTREAM programmes, because US law itself contains no significant safeguards in relation to communications outside the US not relating to US persons (see statement of Cindy Cohn at §§54-55, 60 **[Annex 1/87-88, 90]**).

In these circumstances the requirements that an interference with Article 8 rights be 'in accordance with the law' are not made out.

In a presentation in 2011, a GCHQ legal adviser told NSA analysts t*hat a reason f*or using TEMPORA material was that, "[the UK] *ha[s] a light oversight regime compared with the US*."13 Indeed, *The Guardian* reported on internal GCHQ documents from 2011 which recorded one of the UK's *"unique selling points" as* being "*the UK's legal regime*", given that GCHQ is "*less constrained by NSA's concerns about compliance*"14.

If there is any statement worthy of examination and investigation, it must be this. I hope our legal action will allow such an examination.

Notwithstanding the leaks relating to the TEMPORA programme, the UK Government has refused to confirm or deny the existence of the program or provide any information about external communications warrants granted (in contrast to the approach of the US Government in respect of the PRISM programme).

Indeed, only a few days ago, the director of the National Security Agency, Gen. Keith B. Alexander, said: "Given where we are and all the issues that are on the table, I do feel it's important to have a public, transparent discussion on cyber so that the American people know what's going on, and in order to have that, they need to understand the truth about what's going on."

Such a sentiment is laudable, although we will wait to see the details of what the American public is told before heralding a new era of transparency.

As we submit in the document outlining the grounds for our claim, what is required is a framework which enables a citizen to understand with sufficient particularity the types of person and conduct in relation to whom surveillance may occur; the safeguards which exist and govern dissemination and sharing of such material; the framework which exists to guard against arbitrary or disproportionate use of such material; and checks on the authority required to permit such surveillance and limits on the time for which such surveillance may occur. What is required is a legal framework which provides an ascertainable check against arbitrary use of secret and intrusive state surveillance.

Around the world, millions of people do not know the same freedom as us. Journalists and political activists are murdered or kept under surveillance. Corruption is rife and elections, if they happen at all, are not free or fair.

Citizens of such nations do not look to their own corrupt, brutal governments for hope. They look to countries like Britain, where a free press can hold our leaders to account and people are free to communicate in private, to meet who they chose and to live their lives without the fear of their most intimate details being pored over by a faceless bureaucrat or unaccountable police officer. They look to us to spread freedom, to defend democracy and to show that an open society is something to aspire to.

When faced with a new threat, we can reach for more curtailment of liberty and surrender a little more freedom in the hope it will make us safer. Or we can stand up and defend the free and open society that those who seek to terrorise us detest. We do not defeat terrorism by abandoning our freedom, we defeat terrorism by spreading freedom, defending liberty and standing tall in the face of those who would seek to do us harm.

Thank you for your time today.