Human Rights Watch
Submission to the Intelligence and Security Committee of Parliament
Privacy and Security Inquiry
February 7, 2014

Dear Committee Members,

Human Rights Watch submits the following information to the Committee's Privacy and Security Inquiry, based on public statements by Human Rights Watch following the publication by the *Guardian* of revelations on surveillance by the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ).[1] Firstly, we highlight the urgent need for clarity from the government as to the scope and magnitude of the alleged surveillance by GCHQ. Secondly, the law governing surveillance must be brought up to date in a way that protects the right to privacy and, thirdly, the government should create a more robust and transparent oversight authority to protect against breaches of that right.

After reports emerged in 2013 that GCHQ had intercepted and collected vast amounts of internet and phone data from people living in the UK and other countries, Human Rights Watch expressed serious concerns that, if those allegations were true, the government had breached the privacy rights of millions of people in the UK and elsewhere.

According to reports in the *Guardian* newspaper, GCHQ accessed enormous quantities of data travelling from North America to and through the UK and shared this data with the US NSA. The data was said to include recordings of phone calls, e-mail contents, and data on the use of websites and social media. The reports suggested that the content of the data was generally stored for up to three days, and that metadata (which for the internet could include information that identifies users, their locations, and their searches) for up to thirty days. It was further suggested that analysts for GCHQ and NSA then filtered through the data, searching for information that was of interest or use to them.

---

[1] Human Rights Watch, "UK: Provide Clear Answers on Data Surveillance – Stronger Legislation, Oversight Needed to Protect Privacy Rights", June 28, 2013, http://www.hrw.org/news/2013/06/28/uk-provide-clear-answers-data-surveillance; Human Rights Watch, Letter to UK Foreign Secretary William Hague – Data Surveillance Claims and Protecting the Right to Privacy, July 1, 2014, http://www.hrw.org/news/2013/07/01/letter-uk-foreign-secretary-william-hague

The *Guardian* reported that the UK intelligence agency had tapped more than 200 cables linking the UK to the global Internet. Because of the UK's location, the majority of transatlantic Internet traffic may flow through the cables the government has access to, including traffic flowing to and from servers of major US-based Internet companies implicated in media reports relating to similar alleged programs operated by the NSA.

The allegations suggest that the legal framework in the UK that regulates such an interception and oversight mechanism is inadequate to protect against wholesale breaches of privacy rights.

While we fully accept that the UK government has a duty to protect national security and prevent crime, there is an important distinction between taking steps that are necessary and proportionate to achieve those aims and monitoring indiscriminately the communications of millions of people in the UK and other countries who are under no suspicion whatsoever.

The UK government should explain to the public the scope and magnitude of the alleged surveillance by the GCHQ as well as the authority and limitations under which it is conducted. The government should also clarify how much data on people located outside British territory is being gathered and how it is being stored, used, or shared with third parties, particularly since the legal protections against such interception is weaker than for people abroad under UK law. If the allegations that GCHQ has been intercepting and collecting data on the citizens of other countries are true, this could have a serious impact on the rights of individuals in the EU (and elsewhere).

Under the European Convention on Human Rights (ECHR), and the Human Rights Act (HRA) which incorporates it into domestic law, the UK must respect the right to private life and any interference with this right must be "in accordance with the law" and "necessary in a democratic society," and it must be proportionate. The greater the potential impact on rights of the exercise of executive discretion, the greater the authorities' duty to ensure there is adequate oversight to guard against abuse.

It is hard to reconcile these principles and legal duties with what is reported about the actions of GCHQ. If the reported allegations are true, the right to privacy of millions of people in and outside the UK has been breached. To date, the government has not presented information that satisfactorily disproves the claims.

Instead, in response to allegations Foreign Secretary William Hague claimed that the existing legal framework is robust and has not been breached, and that no further

information can be provided to the public. Hague tried to close down debate by saying that he will not comment on intelligence operations. The Foreign Secretary has also defended intelligence sharing between the UK and the US, saying that in both countries intelligence work operates under the rule of law.

After the media disclosed information about GCHQ's involvement in US secret surveillance programs, Hague told Parliament that warrants he and other senior ministers grant for GCHQ operations "are legally required to be necessary, proportionate and carefully targeted, and we judge them on that basis." The revelations by the *Guardian* would appear to directly contradict this assertion.

Human Rights Watch holds that the government needs to give a clear explanation about these claims and about how the law is being applied.

Furthermore, **the government should bring up to date the law under which GCHQ has been acting**, namely the Regulation of Investigatory Powers Act 2000 (RIPA). In the thirteen years since the UK's new law on intercepting communications was introduced, technology has obviously evolved very dramatically and the government now has the duty to reassess the legal framework to ensure that the right to privacy is upheld.

RIPA allows a senior government minister—a "secretary of state"—to issue a warrant at the request of a senior intelligence or police official. The warrant authorizes the interception of communications for which the sender or intended recipient is in the United Kingdom, if the secretary of state believes intercepting the information is necessary and proportionate.

The grounds for granting a warrant under the law are extremely broad. In addition to permitting a warrant if it is "necessary" "in the interests of national security," the law permits a warrant if it is "necessary" for "preventing or detecting serious crime" or "safeguarding the economic well-being of the United Kingdom."

Section 8(4) of the law also allows a senior government minister to issue a certificate that allows granting a warrant to intercept communications sent or received outside the "British Islands"—the UK, plus Jersey, Guernsey, and the Isle of Man—without specifying a named person or premises. *The Guardian* suggests that the foreign secretary has relied on that provision to justify intercepting fiber-optic communications since these cables carry traffic from abroad. In issuing the certificate, the secretary of state must confirm that the interception is "necessary" for a legitimate purpose under the law and provide a description of the material it is necessary to examine. However, it is unclear how specific the description contained in the certification must be.

In addition, because a significant portion of Internet traffic between two people in the UK may be routed abroad, such traffic could also be intercepted under the lower standard for communication outside the UK.

The government should treat the privacy rights of individuals whose communications it intercepts in the same way whether they are inside or outside the UK. When a country can exercise control or jurisdiction over the digital communications of non-citizens, or people outside its borders, in a comprehensive or wholesale fashion, it also assumes an obligation to respect those people's rights.

Also, **the government should create a more robust and transparent oversight authority** that reports to Parliament. This agency should be mandated to disclose as much information to the public as possible, consistent with the requirements of national security and public order.

Human Rights Watch believes that the existing oversight and accountability mechanisms in this area are not adequate to prevent abuse of surveillance powers, and are not consistent with the UK's human rights obligations.

Once the communications have been intercepted, RIPA provides very weak safeguards for the use of material that relates to people located outside the "British Islands." Oversight under RIPA is neither transparent nor comprehensive. The interception of communications commissioner has oversight of the government's power to intercept, but the prime minister, not the parliament, appoints the commissioner. The commissioner examines a number of interception warrants after the fact and assesses whether they comply with the criteria of necessity and proportionality, but does not reveal how many warrants are inspected or what proportion of warrants issued these constitute, or whether the warrants inspected are representative of the scope and varieties of warrants as a whole. The commissioner's annual report—for which the prime minister must approve the content—suggests that the selection is largely made at random.

A person who believes one of the intelligence agencies has breached their right to privacy this way can file a complaint before the Investigatory Powers Tribunal, a judicial body. The tribunal can quash the interception warrant and order the records collected to be destroyed or award compensation. But if it doesn't uphold the person's claim, it doesn't let the person know whether an interception took place, and the tribunal's decisions cannot be challenged in court.

Any new legislation should ensure that communications data is intercepted only

in exceptional circumstances and that any decision authorizing such interception is subjected to independent scrutiny by a judicial authority. The law needs to be clear on what is authorized and for what purpose, and avoid broad categories such as "the interests of national security" or "the economic well-being of the United Kingdom."

In a recent report, the UN special rapporteur on the right to freedom of expression and opinion, Frank La Rue, urged countries to regard communications surveillance as "a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society." He warned that "[i]nadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression."