PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

The Rt Hon Theresa May MP
Prime Minister
10 Downing Street
London SW1A 2AA

11 May 2018

Dear Prime Minister,

RE: Abdel Hakim Belhaj and Fatima Boudchar - Intelligence Sharing and Human Rights Concerns

Following your unprecedented apology (10 May 2018) in Parliament, which accepts that the UK's actions contributed to Abdel Hakim Belhaj and Fatima Boudchar's detention, rendition and suffering and that the UK government "*shared information about [them] with its international partners*" and "*should have done more to reduce the risk that [they] would be mistreated*", we are writing to express our concerns regarding the lack of safeguards governing the UK's intelligence sharing arrangements with international partners. We recommend that the Government now prioritise urgent reforms for improving oversight of intelligence sharing. We believe that without such reforms, public confidence in the current system will be severely undermined.

We believe you must urgently:

- Make public existing intelligence sharing arrangements
- Make public all relevant rules and policies governing intelligence sharing
- Establish, through primary legislation, a legal framework governing intelligence sharing, which provides for sufficient safeguards and oversight of intelligence sharing
- Implement safeguards to address nearly unfettered powers for cross-border transfers of personal data by intelligence agencies in Part 4 of the Data Protection Bill

Human Rights Risks of Intelligence Sharing

Intelligence sharing constitutes an interference with the right to privacy and must therefore be subject to safeguards that are well-established in international human rights law, which include adequate oversight. As appears to have happened here, unregulated intelligence sharing can contribute to or facilitate serious human rights abuses, such as unlawful arrest or detention, or torture and other cruel, inhuman or degrading treatment. Without appropriate safeguards, states can also use intelligence sharing to 'outsource' surveillance, bypassing domestic constraints on their surveillance activities.

UK Intelligence Sharing Arrangements

We call on you to make public existing intelligence sharing arrangements.
In the UK, intelligence agencies share large amounts of intelligence with foreign agencies under various arrangements. The most important, the Five Eyes alliance (made up of the UK, US, Canada, Australia and New Zealand), was formed shortly after World War II. A 1956 version of the governing agreement – the UK-US Communication Intelligence Agreement – is the most recent version of the agreement to have been made public. It provides that the Five Eyes agencies will share, by default, all raw signals intelligence and also techniques related to the acquisition of such intelligence. Communications technologies as well as the nature of signals intelligence have changed dramatically since 1956.

Over the last few years, information about the nature and scope of the information shared pursuant to the Five Eyes alliance has been revealed in the public domain. The media has reported, for example, that data flowing through undersea cables that land in the UK are intercepted by GCHQ and made accessible to the NSA, and also that GCHQ has access to a database containing the content and metadata of hundreds of millions of text messages collected by the NSA. It has further revealed that the UK and US (as well as a number of other countries) each have access to a network of servers storing information acquired under various programs operated by their respective intelligence agencies.

The UK also reportedly allows US intelligence agencies to collect intelligence from within the UK on military bases, including in support of special operations involving lethal force.

The UK may be party to many other intelligence sharing arrangements. Due to the secrecy shrouding these arrangements, the public is unaware of the other governments with which the UK shares intelligence, let alone the rules governing such sharing. Improving oversight is a matter of urgency for the British public. In a 2017 YouGov poll carried out by Privacy International, 78% of British people

said they do not trust the US President Donald Trump to only use surveillance powers for legitimate reasons. There is widespread concern that Trump will also use his powers for personal gain. Three quarters of Britons want the UK Government to tell the public what safeguards exist to stop Trump from misusing their data.

Last month, we released an analysis based on an international collaborative investigation carried out by 40 NGOs in 42 countries which found alarming weaknesses in oversight arrangements that are supposed to govern the sharing of intelligence between governments, including between the UK and foreign intelligence agencies. Please find attached the full report outlining our analysis, findings, and recommendations for improving the oversight of international intelligence sharing in the UK.

We submit that the minimal information in the public domain is unacceptable. Non-transparent, unfettered and unaccountable intelligence sharing threatens the foundations of the human rights legal framework and the rule of law.

A Legal Framework Governing Intelligence Sharing

We call on you to establish, through primary legislation, a legal framework governing intelligence sharing, which provides for sufficient safeguards and oversight of intelligence sharing

When the Investigatory Powers Bill was announced, the Home Secretary said that it was about "*strengthening the safeguards, and establishing a world-leading oversight regime*", but the Act sets a poor example with respect to regulating intelligence sharing. For example, the Act focuses on "*requests*" to exchange intelligence with foreign partners and does not address other forms of intelligence sharing, such as the UK's direct and unfettered access to raw data intercepted in bulk or databases of material collected in bulk by foreign governments. The Act also fails to provide adequate safeguards or oversight of intelligence sharing. It does not address, for instance, whether international and domestic legal constraints applying to direct surveillance apply equally to information obtained through intelligence sharing. It continues to leave the public substantially in the dark as to the circumstances in which intelligence agencies will share information and the procedures governing such sharing.

In 2015, the UN Human Rights Committee, when reviewing the UK's implementation of its obligations under the International Covenant on Civil and Political Rights, expressed concerns "*about the lack of sufficient safeguards in regard to the obtaining of private communications from foreign security agencies and the sharing of personal communications data with such agencies*" and

recommended "*robust oversight systems over...intelligence-sharing of personal communications activities..., including by providing for judicial involvement in the authorization of such measures in all cases*". This recommendation remains unfulfilled.

Ensure Data Protection Safeguards

We call on you to address the nearly unfettered powers for cross-border transfers of personal data by intelligence agencies in Part 4 of the Data Protection Bill.

Part 4 of the Bill covers data processing by intelligence agencies and is based on the Council of Europe's draft Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Clause 109 of Part 4 of the Bill provides for transfers of personal data outside the UK by the intelligence agencies. However, it fails to provide an appropriate level of protection as required by Article 12 of Convention 108. Further, Clause 109 provides lower safeguards than those applicable to law enforcement transfers of personal data in Part 3 of the Bill.

The only condition in Clause 109 – namely that such transfers are necessary and proportionate for the purposes of the controller's statutory functions or for other purposes as provided in the Security Services Act 1989 or Intelligence Services Act 1994 – does not provide meaningful safeguards as these purposes are overly vague and broad. As such, Clause 109 does not provide for an appropriate level of protection as demanded by Article 12 of Convention 108, which this clause is said to implement.

We attach our briefing on the Data Protection Bill noting pages 21 – 22.

***

In your apology yesterday you acknowledged that the government "*should have done more to reduce the risk*" of Abdel Hakim Belhaj and Fatima Boudchar's mistreatment. Regulating and establishing independent oversight of intelligence sharing would be significant steps to reduce the risk of the UK's complicity in serious human rights violations.

In light of the apology made to Abdel Hakim Belhaj and Fatima Boudchar and your acceptance that the UK should have done more to reduce the risk of mistreatment following the sharing of intelligence, we again ask you to confirm that:

- You will make public existing intelligence sharing arrangements – including the text of the current version of the agreement governing the Five Eyes alliance
- You will make public all relevant rules and policies governing intelligence sharing.
- You will establish, through primary legislation, a legal framework governing intelligence sharing, which requires *inter alia*:
    - All intelligence sharing agreements to be subject to approval by both executive and legislative bodies, and to be presumptively public;
    - Intelligence sharing agreements to permit oversight bodies to have access to information provided to and received from a foreign partner;
    - International and domestic legal constraints that apply to direct surveillance by intelligence agencies also apply equally to information obtained through intelligence sharing arrangements;
    - Prior independent authorisation for sharing intelligence with a foreign partner;
    - Transparency as to the circumstances in which intelligence agencies will share information and the procedures governing such sharing, including limiting sharing to where it is in accordance with law, necessary and proportionate, and articulating the process for authorising sharing;
    - Regular audits of how foreign partners store, manage and use the information that has been shared, and examination of financial resources allocated to intelligence sharing, including for providing equipment and training to foreign partners.
- You will ensure essential data protection safeguards addressing the nearly unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection, as set out in Part 4 of the Data Protection Bill.

We look forward to a prompt response. Please do not hesitate to contact us if you have any questions.

Your sincerely,



Scarlet Kim
Legal Officer