PRIVACY INTERNATIONAL

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

Rt Hon Sajid Javid MP
Home Secretary
Home Office
2 Marsham Street
London
SW1P 4DF

Sent by email: public.enquiries@homeoffice.gsi.gov.uk

CC: Investigatory Powers Tribunal

25 September 2018

Dear Sajid Javid

We are writing to express our grave concern and to request your urgent action following today's disclosures regarding the interception of data by the Security and Intelligence Agencies (SIA), including their alarming acquisition and retention of data relating to Privacy International and/or its employees.

Privacy International (PI) is a registered charity based in London that works at the intersection of modern technologies and rights. Privacy International challenges overreaching state and corporate surveillance, so that people everywhere can have greater security and freedom through greater personal privacy.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs et al.

As you will be aware, in June 2015 PI commenced a challenge at the Investigatory Powers Tribunal against the Foreign Secretary, the Home Secretary and the SIA regarding the acquisition, use, retention, disclosure, storage and deletion of 'Bulk Personal Datasets' (BPDs) and Bulk Communications Data (BCDs).

These databases and datasets contain vast amounts of personal data about individuals, the majority of whom are unlikely to be of intelligence interest. For example, BPDs held by the SIA include passport databases, travel data, and finance-related activity of individuals, while BCDs (the "who, when, where, and how" of both telephone and internet use) include location information and call data for everyone's mobile telephones in the UK for 1 year.

Our challenge has resulted in important public disclosures and avowals. In October 2016, the Tribunal held that the SIA had breached Article 8(2) of the European Convention of Human Rights in respect of both the BPD and BCD regimes. The Tribunal held that, from their commencement over a decade earlier until their public avowal in 2015, there was not sufficient foreseeability or accessibility of the existence of the BPD and BCD regimes, nor of the nature of controls over them; in consequence, the regimes could not be said to be "in accordance with law".

In July 2018, the Tribunal found that granting unfettered discretion to GCHQ to determine what data to acquire from telecommunication companies was an unlawful delegation of power from the Foreign Secretary. The government had initially claimed that the Foreign Secretary had direct and full control over what data telecommunications companies had to provide to GCHQ. But upon further information coming to light, it instead argued that the Foreign Secretary could lawfully choose to delegate to GCHQ decisions about what data to acquire from telecommunication companies. The result of the judgment is that a decade's worth of secret data capture has been held to be unlawful.

This unlawfulness would have remained a secret but for Privacy International's work. During the hearing, the Tribunal praised Privacy International's legal team for its dedication and valuable inquisitiveness, whilst also noting the constant necessity of both Privacy International and Counsel for the Tribunal to probe and consider fresh problems and lacunae.

Today's Hearing

On 12 December 2016, the Tribunal ordered the SIA to carry out searches of their databases (including BCD and BPD) for identifiers related to Privacy International and to provide a report detailing the results of those searches. On 17 February 2017, the SIA responded and confirmed that both the Security Service and Secret Intelligence Service search results showed that they held data relating to Privacy International in their BPDs prior to their avowal on 12 March 2015. The February report stated that neither GCHQ nor the Security Service's searches revealed any relevant BCD.

In 6 October 2017, the report was amended for the first time, to show that the Security Service did, in fact, hold relevant data in its BCDs prior to their avowal on 4 November 2015.

In conjunction with its 23 July 2018 judgment, the Tribunal ordered the SIA to prepare a revised search report to cover the new time period during which GCHQ's BCD regime violated art 8(2), which was extended until 14 October 2016. As a result, the search report was re-amended, and now confirms that:

- All three of the agencies held (or, in the case of GCHQ, more likely than not held) data relating to Privacy International in its BPDs while the BPD regime was unlawful

- Both GCHQ and the Security Service held data relating to Privacy International its BCDs while the BCD regime was unlawful.
- The Security Service acquired and selected for analysis data relating to Privacy International as part of one or more investigations, and stored it in an area which stores the results from searches which officers have undertaken. This data was stored indefinitely, with no period for its review and deletion.

We are extremely concerned that Privacy International data has been caught up in an active investigation by MI5. In addition, it is a matter of concern that this:

- Was not discovered in the initial searches;
- Was only discovered in circumstances that are entirely unexplained (the Tribunal is invited to direct the production of a witness statement providing an explanation); and
- Demonstrates that the Agencies are unable to identify accurately and in a timely fashion what data they hold and where they hold it, and give a comprehensive and accurate statement to the IPT as to what is held.

We have not yet seen the full relevant evidence. The reports on searches have not yet been through the full disclosure process and we consider that further material ought to be disclosed.

Big Brother Watch and Others v. the United Kingdom

As you will be aware, last week the European Court of Human Rights (ECtHR) issued its judgment in Big Brother Watch and Others v. the United Kingdom. The case concerned the UK's mass interception of internet-based communications and the SIA's access to intelligence gathered by other governments' surveillance programs, including the mass surveillance programs of the U.S. National Security Agency ("NSA").

The Court ruled that the UK government's mass interception program violates the right to privacy, holding that the program "is incapable of keeping the 'interference' [with such rights] to what is 'necessary in a democratic society'". Specifically, the Court found the legal regime (pursuant to section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA")) governing that interception violated the right to privacy as enshrined in Article 8 of the European Convention on Human Rights (ECHR). (§§ 387-388) The Court expressed specific concern over the way in which the UK government selects the undersea cables it will tap (called "bearers" by the Court), and the search criteria applied to the communications obtained from those cables.

The Court stated that it was "not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse." It also emphasised that what was "[o]f greatest concern...is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications." (§ 347). The Court

also criticised the UK regime's "absence of any real safeguards applicable to the selection of related communications data for examination." (§387).

The Court also extended and amplified its concerns about the UK's mass interception program in addressing its impact on journalists, noting that in the freedom of expression context, "it is of particular concern that there are no [public] requirements...either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved." (§ 493). The Court recognised that such a blanket power to interfere with journalists' communications, including with their sources, could have a broader "chilling effect...on the freedom of the press." (§ 495).

Your Urgent Action is Required

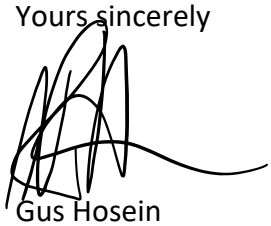
The Investigatory Powers Act (IPA) does not address the Court's concerns. On its face, the IPA does not provide for any oversight of the selection of bearers or search criteria applied to the communications obtained through mass interception. In particular, the IPA does not require any oversight at the stage at which search criteria are applied. In addition, the government needs to revisit the IPA provisions governing how the SIA examine communications data related to intercepted communications and provide for strengthened safeguards.

We are therefore writing to ask that you to:

- Confirm what changes you will make to the IPA as a result of last week's ECHR judgement;
- Instruct the SIA to provide to our Counsel and ourselves a full explanation as to why the SIA unlawfully held and analysed Privacy International's data; and
- Confirm whether you will take any action, including the prioritisation of additional safeguards and oversight measures, to ensure that charities operating in the public interest are not subject to unlawful surveillance by the SIA.

We look forward to a response as a matter of urgency.

Yours sincerely



Gus Hosein
Executive Director