**RESPONSE OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND**

**TO THE CALL BY THE SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION**

**FOR CONTRIBUTIONS TO HIS REPORT ON**

**THE SURVEILLANCE INDUSTRY AND HUMAN RIGHTS**

1. **Information concerning the domestic regulatory frameworks that may be applicable to the development, marketing, export, deployment, and/or facilitation of surveillance technologies by private companies, such as:**
   1. Laws, administrative regulations, judicial decisions, or other policies and measures that impose regulations on the export, import or use of surveillance technology;

UK Export Controls

The purpose of UK export controls is to promote global security and facilitate responsible exports. The UK Government controls a range of military and “dual-use”[[1]](#footnote-1) exports, depending on the nature and destination of exports. When considering UK export controls, we take into account:

* Concerns about internal repression, regional instability or other human rights violations.
* Concerns about the development of weapons of mass destruction.
* Foreign policy and international treaty commitments including those resulting from the imposition of EU or United Nations trade sanctions or arms embargoes.
* The need to ensure the national and collective security of the UK and its allies.

The Export Control Act (2002)[[2]](#footnote-2) and the Export Control Order (2008)[[3]](#footnote-3) provide the legal framework for export controls. Dual-use goods, which include items that can be considered to be “Surveillance Technologies”, are covered by EU legislation, specifically Council Regulation (EC) No 428/2009,[[4]](#footnote-4) which is directly applicable in the UK.

Responsibility for Export Controls

The Department for International Trade (DIT) has overall responsibility for the export licensing process. The International Trade Secretary is ultimately responsible for:

* The statutory and regulatory framework of the controls (i.e. what items and activities are controlled); and
* The decision to grant or refuse an export licence in any individual case.

The UK’s system of export controls is administered within DIT by the Export Control Joint Unit.

“Surveillance Technology” Controls

Surveillance equipment can be considered to be equipment covered by the following control entries specified in Annex I of Council Regulation (EC) No 428/2009:

* 5A001.f - Mobile telecommunications interception or jamming equipment
* 5A001.j – Internet Protocol (IP) Network Surveillance Systems
* 5D001.a, 5D001.c and 5E001: Software or technology related to 5A001.f and 5A001.j
* 4A005, 4D004, 4E001a, 4E001c – "Intrusion software" items and related software and technology

These implement controls originating from the Wassenaar Arrangement.[[5]](#footnote-5)

Export Control Policy

The UK Government takes its export control responsibilities very seriously and operates one of the most robust export control regimes in the world.

All export licence applications are assessed on a case-by-case basis against the Consolidated EU and National Arms Export Licensing Criteria,[[6]](#footnote-6) known as the Consolidated Criteria. We draw on all available information, including reports from Non-Governmental Organisations (NGOs) and our overseas network.

The Consolidated Criteria provide a thorough risk assessment framework for assessing export licence applications and require us to thoroughly consider the impact of providing equipment and its capabilities.

We will not license the export of equipment where to do so would be inconsistent with the Consolidated Criteria, including under Criterion 2, which considers the respect for human rights and fundamental freedoms in the country of final destination.

Transparency

The UK Government operates one of the mosttransparent systems of export controls in the world. Every three months the UK Government publishes comprehensive data[[7]](#footnote-7) about licences issued, or refused, and publishes an annual report covering a wide range of policy issues related to export controls. This reporting conforms to the Government’s Code of Practice for Official Statistics, which provide a high level of quality assurance.

Use of Surveillance Technology and Data Protection

Most uses of surveillance technologies by private companies (for example, CCTV in business premises) will be covered by the EU General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The GDPR gives data subjects the right to see any personal data held about them (including CCTV images).

It also sets rules for all data controllers, including CCTV operators, about the circumstances in which they can gather, store and disclose personal data. The Information Commissioner and independent regulator enforce these rules in the UK.

The Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016

The use by relevant UK public authorities of investigatory powers, including surveillance, is covered by legislation such as the Regulation of Investigatory Powers Act 2000, and the Investigatory Powers Act 2016. The Act also maintains the offence of interception of communications without lawful authority, which applies to any person who unlawfully intercepts communications in the UK.

The Security Industry Authority

Within the UK, there is a statutory organisation that is responsible for regulating the private security industry, this is the Security Industry Authority (SIA). It is a non-departmental public body, established in 2003, and the SIA reports to the Home Secretary under the terms of the Private Security Industry Act (2001). The full legislation can be found here: <http://www.legislation.gov.uk/ukpga/2001/12/contents>.

The purpose of the SIA is to regulate the private security industry effectively, to reduce criminality, raise standards, and recognise quality service. It has two main functions:

* The compulsory licensing of individuals undertaking designated activities, including public space surveillance (CCTV). A CCTV licence is required when manned guarding activities are carried out through the use of closed circuit television equipment to (i) monitor the activities of a member of the public in a public or private place; or (ii) identify a particular person; and
* Managing the voluntary Approved Contractor Scheme, which measures private security suppliers against independently assessed criteria.
  1. Remedies available in the event of illicit export or use of private surveillance technology;

Illicit Export

The Export Control Order 2008 contains offences for exporting controlled goods without a licence. The maximum penalties on conviction on indictment are ten years imprisonment and an unlimited fine. Her Majesty's Revenue and Customs does not view a criminal prosecution as the only successful law enforcement outcome in all cases. Our objective is to use a spectrum of interventions that drive changes in non-compliant behaviour in accordance with our compliance strategy (Promote / Prevent / Respond). There are several other options we can and regularly do exercise besides criminal prosecutions. These can include awareness, warning letters, issuing compound penalties and seizure / disruption actions.

Data Protection

The Information Commissioner is responsible for enforcing the UK's data protection legislation. A person who considers that an organisation has used his or her personal data in a way which is not permitted by the GDPR can complain to the Information Commissioner. Organisations can be fined up to £20 million euros or 4% of their annual turnover (whichever is higher) for breaches of the GDPR. Data controllers can appeal (to the First Tier Tribunal) if they consider that the Information Commissioner has used her investigatory and enforcement powers incorrectly.

The Security Industry Authority

To obtain an SIA licence, individuals are checked. This involves checks on identity, right to work, and historical criminal records. All operatives are required to complete a training qualification specified by the SIA. Every time there is a licence application, including licence renewals, there is a criminal records check. A criminal record will not necessarily preclude someone from holding an SIA licence, but this is dependent on the type and seriousness of the offence(s), the sentence/disposal received, and how long ago it was. The criminality criteria were developed in line with the rehabilitation periods in the Rehabilitation of Offenders Act 1974.

The licensing conditions are clear that all security operatives must tell the SIA as soon as practicable of any convictions, cautions or warnings, or charges for relevant offences whether committed in the UK or abroad. Should a licence-holder do anything that means they fail to comply with the licensing conditions the matter will be investigated. When notified of any convictions, cautions or warnings, or charges, the SIA review this against the licensing criteria and consider whether a security operative should retain their licence or if it should be suspended or revoked.

* 1. Whether the laws, regulations, or policies identified are consistent with State obligations under Article 19 of the International Covenant on Civil and Political Rights, Article 19 of the Universal Declaration of Human Rights, and other relevant human rights standards.

UK policies are consistent with State obligations under Article 19 of the International Covenant on Civil and Political Rights and other obligations including article 10 of the European Convention on Human Rights, to the extent that the laws, regulations and policies engage with those obligations. They are also consistent with Article 19 of the Universal Declaration of Human Rights, and other relevant human rights standards.

1. **Information concerning the use of such surveillance technologies:**
   * 1. Details of emblematic cases of State use of private surveillance technology against individuals or civil society organizations.

The use by relevant UK public authorities of investigatory powers, including surveillance, is covered by legislation such as the Regulation of Investigatory Powers Act 2000, and the Investigatory Powers Act 2016. These powers may only be used where it is necessary and proportionate to do so. The use of such powers is overseen by the Investigatory Powers Commissioner (IPC), who reports annually to the Prime Minister. The IPC is supported by a team of independent Judicial Commissioners who, alongside the IPC, are responsible for overseeing the use of investigatory powers by public authorities. They are supported in this work by a body of officials – the Investigatory Powers Commissioner’s Office (IPCO).[[8]](#footnote-8) Previous annuals reports, including details of investigations of serious errors and breaches, are available on the publications page of the IPCO website.[[9]](#footnote-9) The IPCO’s first report was published online in January 2019.

* + 1. Company policies to ensure that the development and sale of surveillance technologies meets human rights standards, particularly those articulated in the UN Guiding Principles on Business and Human Rights.
    2. The extent to which private surveillance companies offer services to States and other actors to deploy their technologies in specific circumstances, and the extent to which companies are aware of the end-use of the technologies they market.
    3. Company standards or policies to monitor the use of their technology after it is sold to governments.

It is for companies to comment on their individual standards and policies. However, the following background on the UK government’s approach may be useful:

In September 2013, the UK became the first UN Member State to develop a National Action Plan to implement the UN Guiding Principles on Business and Human Rights. In order to reflect actions taken by the Government, the Action Plan was updated in 2016 and set out the role the Government will play in helping business to fulfil its responsibility to respect human rights. The updated Action Plan is published on the UK Government’s Website.[[10]](#footnote-10) The UK Government believes in the importance of the business and human rights agenda and that the promotion of business and respect for human rights go hand in hand.

The UK is committed to fully implementing the UN Guiding Principles on Business and Human Rights. The UK Government has encouraged other countries to follow our example by creating and implementing their own National Action Plans, which will in turn allow for greater respect for human rights across the world of business.

We work through intergovernmental institutions, including the EU, to encourage and support companies to meet their obligations and responsibilities in the prevention of human rights abuses.

The Government has helped to develop an increased emphasis within the business community on the importance of reporting, benchmarking companies’ social and ethical performance, and corporate transparency. This has included:

* Clarifying legislation to ensure that eligible companies are required to report on human rights as part of their annual strategic reports;
* Transposing the EU non-financial reporting Directive 2014/95/EU to enable greater consistency and comparability of public information on the human rights policies and performance of listed companies in Europe;
* Supporting the development of the UN Guiding Principles Reporting Framework; a comprehensive tool including guidance for companies to report on human rights issues in line with their responsibility to respect human rights; and
* Supporting the development of the Corporate Human Rights Benchmark, which seeks to rank the top 500 globally listed companies on their human rights policies, processes and performance.

The UK also played a leading role in the drafting of the International Code of Conduct for Private Security Providers (ICoC) and the launch of its oversight mechanism, the International Code of Conduct Association (ICoCA) in 2013. ICoCA is a multi-stakeholder initiative made up of three pillars: governments, Private Security Companies (PSCs) and civil society organisations. ICoCA aims to raise standards in the international PSCs sector via a system of certification, monitoring and complaints functions. The UK sits on ICoCA’s Board of Directors. We encourage all states, companies and NGOs that contract PSCs to recognise ICoCA membership and certification to relevant standards in their contracting processes.

15 February 2019

1. Dual-use items are goods, software, technology, documents and diagrams, which can be used for both civil and military applications. They can range from raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. They could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers. [↑](#footnote-ref-1)
2. <http://www.legislation.gov.uk/ukpga/2002/28/contents> [↑](#footnote-ref-2)
3. <http://www.legislation.gov.uk/uksi/2008/3231/contents/made> [↑](#footnote-ref-3)
4. [https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF](https://emea01.safelinks.protection.outlook.com/?url=https%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DOJ%3AL%3A2009%3A134%3A0001%3A0269%3Aen%3APDF&data=02%7C01%7Cdean.gallacher%40trade.gov.uk%7C6eff014dd88b44e366c208d67d39ea70%7C8fa217ec33aa46fbad96dfe68006bb86%7C0%7C0%7C636834086000043940&sdata=IWFDDuyphdQepHjM6xOPVLcs1%2FyODMq4EvKZn%2BepZxQ%3D&reserved=0) [↑](#footnote-ref-4)
5. <https://www.wassenaar.org/> [↑](#footnote-ref-5)
6. <https://publications.parliament.uk/pa/cm201314/cmhansrd/cm140325/wmstext/140325m0001.htm> [↑](#footnote-ref-6)
7. <https://www.gov.uk/government/collections/strategic-export-controls-licensing-data> [↑](#footnote-ref-7)
8. The Investigatory Powers Commissioner replaced the Intelligence Commissioner, the Interception of Communications Commissioner, and the Chief Surveillance Commissioner. [↑](#footnote-ref-8)
9. <https://www.ipco.org.uk/> [↑](#footnote-ref-9)
10. <https://www.gov.uk/government/publications/bhr-action-plan> [↑](#footnote-ref-10)