SURVEILLANCE *AND BREXIT*

OPEN RIGHTS GROUP BRIEF

OPEN RIGHTS GROUP

Issue

The practice of mass surveillance made headlines in 2013 when Edward Snowden exposed the widespread scale on which the UK security agency GCHQ was covertly intercepting and monitoring citizens' private communications data. Although subsequent court rulings consistently held that this bulk data collection scheme was operating in a manner that breached fundamental rights to privacy, legislation enacted by the government to consolidate its surveillance powers means that the UK currently has the one of the most sweeping and intrusive state surveillance regimes in the Western democratic world.

Open Rights Group has fought to ensure that the right to privacy is respected by the UK, including through bringing litigation that has changed the course of fundamental rights.

Post-Brexit, the UK has the opportunity to re-examine its surveillance operations and could potentially extend them beyond EU restrictions. However, the UK will remain linked to EU privacy and data protection standards and its actions must fully comply with fundamental rights.

State surveillance, data retention and the EU

Articles 7 and 8 of the Charter for Fundamental Rights of the European Union guarantee rights to respect for private communications and protection of personal data. EU protection of these rights, however, is limited by Member State assertions of the need to collect, retain and share data in order to combat serious crime including terrorism.

State surveillance laws and policies are reserved sovereign matters for Member States. States can justify certain levels of citizen surveillance for legitimate law enforcement purposes; however, measures taken must always be necessary and proportionate.

EU INSTITUTIONS AND LAWS

The EU has a strong framework of security and law enforcement institutions, including Europol, an agency coordinating policing across Member States. EU Member States' strategic cooperation on policing and intelligence involves active sharing of citizen data with Europol, which in turn retains this in a vast, centralised database.

With a strong push from the UK after the London terror attacks, in 2006 the EU passed the Data Retention Directive. This required national providers of public communications networks to monitor all of their citizens' digital communications traffic and location data and retain this for a period between six and twenty-four months. This data reveals e.g. what websites people have visited and where they have made telephone calls from and to whom. Through existing framework agreements, Europol and other EU policing and intelligence agencies had real-time access to this data, without limit or oversight.

The Data Retention Directive was struck down by the Court of Justice of the European Union ("CJEU") in the case of Digital Rights Ireland (2014). The Court stated that states could retain certain personal data to combat serious crime but retention schemes had to have clear and precise rules and limits and safeguards to protect data against unlawful access and use and the risk of abuse.

At present, no EU directive or regulation governs national data retention schemes.

EU oversight of UK surveillance law

In response to the case of Digital Rights Ireland, the UK enacted the Data Retention and Investigatory Powers Act 2014 ("DRIPA"). This required public telecommunications operators, when directed by the Home Office, to retain all of their communications data for up to 12 months.

The CJEU reviewed DRIPA in the case of Tele2/ Watson (2016). It ruled that only targeted retention of communications data for the objective of investigating serious crime could be lawful, and requests for data access must be subject to prior review by a Court or other independent body. In line with this ruling, in January 2018 the UK Court of Appeal ruled that DRIPA breached EU law.

In the meantime, however, DRIPA had been replaced by the Investigatory Powers Act 2016 ("IP Act"), widely dubbed a "snoopers charter" by civil liberties groups. The

IP Act is currently being challenged in the UK High Court on the basis that it continues to give a wide range of government agencies powers to bulk collect electronic communications and records of internet use without adequate limits and safeguards.

The Impact of Brexit

After the United Kingdom (UK) leaves the EU:

- For data to continue to flow freely between the UK and the EU the UK will have to seek an "adequacy decision" from the European Commission which determines whether the UK provides citizens with an adequate level of data protection equivalent to that provided within the EU.

In September 2018, the European Court of Human Rights ruled that the UK's mass data interception and retention programmes were incompatible with fundamental rights. The case is under appeal to the Grand Chamber, with a hearing due in July 2019. The court's judgment and the UK government's response will play a role in the EU's adequacy assessment.

The UK's "Five Eyes" intelligence-sharing capabilities may also face new levels of EU scrutiny during the adequacy process. UK legislation and sharing policies that are incompatible with fundamental rights and data protection could stop or limit data flows between EU and UK agencies and organisations.

- The Charter of Fundamental Rights will not apply in the UK and the CJEU will no longer have jurisdiction to decide cases referred to it by UK courts. UK courts will be able to refer to previous (and possibly future) CJEU decisions, however, as standards developed by the CJEU are to be read as if they were references to fundamental rights or principles.

- The judgment in Tele2/Watson (2016) stipulated that retained data for surveillance purposes must remain in the EU. What this means in the context of Brexit is unclear and will be dealt with in an ongoing CJEU case brought by Privacy International and the Investigatory Powers Tribunal.

- The UK will remain a member of the Council of Europe (separate to the EU) and bound by the European Convention on Human Rights ("ECHR"), which protects the right to privacy at Article 8. Open Rights Group is currently challenging the UK's mass surveillance powers and operations before the Grand Chamber of the European Court of Human Rights.

What the Government has said

"It [The future security partnership] must be respectful of the sovereignty of both the UK and the EU's legal orders. So, for example...the UK will respect the remit of the European Court of Justice.

And a principled but pragmatic solution to close legal co-operation will be needed to respect our unique status as a third country with our own sovereign legal order."

Theresa May, 17 February 2018, Speech at Munich Security Conference

The proposals suggest a very close UK-EU cooperation with a mention of respecting the UK's sovereign legal order - although what that respect means in practice is unclear. Additionally, the UK envisages safeguards including robust governance arrangements, a dispute resolution mechanism and a mutual commitment to individuals' rights on the basis of the UK remaining a party to the ECHR after it has left the EU.

This means that the UK may choose not to diverge far from EU policy regarding surveillance and data retention so as to maintain equal standards of protection and regulation.

What ORG wants to see

The UK government should:

- Conduct a full analysis of whether data retention and surveillance laws satisfactorily balance fundamental rights to privacy and data protection against interferences by surveillance measures for national security purposes, including assessing whether they meet ECHR standards, and taking appropriate remedial steps where policies do not meet these standards.

- Fully comply with any legal judgments determining whether it breaches EU citizens' fundamental rights to retain their personal data outside the EU.

UK courts should exercise full powers to review, read down and challenge surveillance/privacy legislation infringing on fundamental rights, including assessing their adequacy against European standards of robust governance.

Open Rights Group (ORG) is the UK's only grassroots campaigning organisation that works to protect your digital rights.

We believe people have the right to control their technology, and oppose the use of technology to control people.

We raise awareness of threats to privacy and free speech and challenge them through public campaigns, legal actions, policy interventions and tech projects.

Open Rights Group

www.openrightsgroup.org

+44 20 7096 1079

Open Rights is a non-profit Company Limited by Guarantee, registered in England and Wales no. 05581537