Britain's mass surveillance regime is directly opposing human rights

April 24 2018, by Matthew White

Credit: LT Chan from Pexels

In light of the Facebook data scandal more people are beginning to

challenge the web's pervasive surveillance culture. But few British citizens seem to be aware of the government's own online surveillance regime – significant parts of which have been deemed unlawful.

The UK government broke EU law under the Data Retention and Investigatory Powers Act (DRIPA), the Court of Appeal ruled in January.

The regime – colloquially known as the Snoopers' Charter – had allowed public bodies to have access to the records of British citizens' web activity and phone records, without any suspicion that a serious crime had been committed. This activity took place without any independent oversight.

DRIPA was rushed through parliament in 2014 by the then Conservative and Liberal Democrat coalition government after the European Court of Justice (CJEU) ruled that the EU-wide Data Retention Directive (DRD) was "invalid", due to the disproportionate levels of mass online surveillance it had allowed countries within the bloc to exploit.

The DRD had required communications service providers to retain subscriber data of their customer base for two years. But the CJEU declared that it seriously interfered with fundamental rights to privacy and data protection in a way that wasn't strictly necessary.

The UK government had justified the swift enactment of DRIPA to patch up what it said was a capability gap, after the DRD was ripped up by the EU, to allow Britain to continue to fight terrorism and other serious crime.

DRIPA allowed secretaries of state to compel telephone companies, internet service providers and web-based services to continue to retain communications data, which concerns the "where, when, with whom and

how".

It works like this, according to the Home Office:

- A person sends an email or text message to someone, the "with whom";
- It reveals "where", in other words the sender's location;
- A time stamp is also provided for "when" the message was sent;
- The communications data also reveals "how" the message was sent, by revealing which messaging service was used;
- It doesn't reveal the content of a message.

In late 2016, DRIPA was replaced by the Investigatory Powers Act (IPA), with many of the same provisions folded into the new law. Then in November 2017 the government acknowledged that, in light of the CJEU's earlier ruling on DRIPA, it would need to amend the IPA to ensure its surveillance regime could be deemed lawful by the EU.

Notably, however, the Court of Appeal's recent ruling on DRIPA took a markedly different approach to the CJEU. It stressed that, while DRIPA had broken EU law, it had not permitted blanket indiscriminate data retention. But my research shows that it is still possible for UK-based operators to be required to retain all data of users and subscribers.

The Court of Appeal also declined to rule specifically on DRIPA because a separate challenge to its successor – the IPA – is underway, even though the government has already conceded that some parts of that legislation are unlawful.

Under the IPA, companies such as BT, Google and Facebook are required to retain communications data on the web activity of anyone for 12 months to allow police, security services and public authorities to access the information. The Home Office has proposed a series of

measures to attempt to fall in to line with EU law, including independent authorisation to approve communications data requests and restricting data retention to "serious crime".

But these apparent concessions have been criticised by campaigners, who argue it is "half-baked".

Human rights law shouldn't be sidestepped

Europe's top courts have made it clear time and again that the continued retention of communications data is a form of mass surveillance.

My research scrutinises the important social ramifications of this surveillance regime now that internet usage is the daily norm for so many people. Communications data can reveal a great deal about online activity: it arguably acts as a kind of internal CCTV.

The mere storage of communications data primarily affects citizens' right to privacy, which is guaranteed by Article 8 of the European Convention on Human Rights and Article 7 of the EU's Charter of Fundamental Rights. This essentially prevents the state from unlawfully, arbitrarily, unfairly, unnecessarily or disproportionately invading a person's privacy.

Privacy is not just an individual right, it has social value, too. According to Alan Westin, who was a professor of public law, privacy "is a prerequisite for liberal democracies because it sets limits on surveillance by acting as a shield for groups and individuals".

Research shows that an inability to protect privacy may result in the failure to defend a democratic state where invasive techniques can swing elections by influencing behaviour.

Privacy also underpins other rights such as freedom of expression, association and religion which are protected by the European Convention on Human Rights.

The Court of Appeal had the opportunity to consistently apply human rights law to the UK's surveillance practices, but instead chose to sidestep the most important issue: whether blanket indiscriminate data retention is human rights compliant – it isn't.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Britain's mass surveillance regime is directly opposing human rights (2018, April 24) retrieved 3 May 2024 from https://phys.org/news/2018-04-britain-mass-surveillance-regime-opposing.html