

Mass surveillance ruled legal in UK

Robert Stevens
17 December 2014

Surveillance of the British population by the UK government spy agencies has been ruled legal by the Investigatory Powers Tribunal (IPT) judicial body.

The IPT has ruled in a case brought by the UK-based Privacy International, Amnesty International and Liberty, as well as the American Civil Liberties Union and Bytes for All (based in Pakistan). They were seeking to establish whether the Tempora surveillance system was a violation of British and international law, specifically Articles 8 and 10 of the European Convention on Human Rights.

In an affront to basic democratic tenets, the ruling allows, in principle, the intelligence agencies to continue to carry out mass surveillance by capturing the data from all fibre optic cables entering or leaving the UK. The IPT ruled the British government was operating according to the Regulation of Investigatory Powers Act (RIPA) 2000.

The case lasted six days and concluded its hearings in July. Five days of the hearings were held in open court, with one day held behind closed doors.

The IPT was created under the RIPA legislation and consists of 10 senior barristers. A thoroughly undemocratic body, it is the only means through which UK citizens can make complains about Government Communications Headquarters (GCHQ) and the other spying operations, MI5 and MI6. The IPT normally meets in secret and is not even required to make a determination on a complaint. Only select IPT rulings are published and its decisions cannot be appealed to a UK court.

Under RIPA, there is legal requirement that intelligence officials acquire a warrant from a minister before performing a wiretap. Privacy International's claim stated, "Through their access to the US programme, UK authorities are able to obtain private information about UK citizens without having to comply with any requirements of RIPA."

Privacy International's claim sought, "A declaration that the Tempora operation under which there is blanket interception, search and storage of data passing through fibre optic cables is unlawful and contrary" to established law, "an order requiring the destruction of any unlawfully obtained material" and an "injunction restraining further unlawful conduct."

The existence of the PRISM and Tempora programmes were among the first revelations to be made public by National Security Agency whistleblower Edward Snowden in 2013. The US government has acknowledged the existence of the NSA's PRISM programme, but the British government will "neither confirm nor deny" Tempora's existence.

The case could only be brought to the IPT on the basis of agreed "hypothetical facts", in an attempt to establish: "If the 'Tempora' mass communications surveillance programme exists, whether it violates the rights to privacy and freedom of expression enshrined in Articles 8 and 10 of the European Convention on Human Rights" and "if the UK government has access to intelligence collected by the [United States] under its PRISM and UPSTREAM programmes, whether that violates Arts 8 and 10 ECHR."

The IPT judgement, in Orwellian language, said it carried out its deliberations, "upon the basis of assuming the relevant allegations to be derived from Mr Snowden's leaks to be true." It continued, "[T]he 'Snowden revelations' in particular have led to the impression voiced in some quarters that the law in some way permits the Intelligence Services carte blanche to do what they will. We are satisfied that this is not the case."

"We have been able to satisfy ourselves that *as of today* there is no contravention of articles 8 and 10 by reference to those systems," the IPT concluded [emphasis added].

The IPT said that it had not yet decided whether or

not the groups bringing the case had had their communications intercepted unlawfully *in the past* and whether any interception discovered was proportionate. The judgment said, “We have left open for further argument the question as to whether prior hereto there has been such a breach.”

Of the numerous surveillance systems exposed by Snowden, Tempora, in operation since 2011, is the largest. He described the Tempora system as the world’s first “full take” surveillance dragnet, meaning that it hoovers up *all* the online activity and communications of the UK population. Tempora is shared with the NSA and GCHQ also has access to NSA databases, which include the data of all UK citizens.

Revealing the first details about Tempora, the *Guardian* noted that as GCHQ infiltrates all the communications in and out of the British Isles, “For the 2 billion users of the world wide web, Tempora represents a window on to their everyday lives, sucking up every form of communication from the fibre-optic cables that ring the world.”

This intrusion is so vast that, for example, GCHQ is able to monitor some 600 million “telephone events” each day. The content gathered from tapped fibre-optic cables is held by GCHQ for three days and the metadata [examples of which include the location from which you last accessed your email or the date and time you called somebody] for 30 days. Both GCHQ and the NSA can search and analyse it with impunity.

The tribunal also ruled, based on secret government policies it was informed of, that the UK can continue to share intelligence with the NSA, or accessing information obtained through the NSA’s PRISM programme.

Commenting on this aspect, Privacy International noted, “The Tribunal also found that the vast intelligence sharing with the NSA and other foreign intelligence and access to the US’ PRISM programme do not contravene the right to privacy despite there being no explicit legislation regulating such activities. In so finding, the Tribunal relied upon the content of secret policies, the existence of which the government was forced to disclose as a result of the IPT claim.”

This was a reference to the fact that during the hearing, Charles Farr, the director general of the Office for Security and Counter-Terrorism, submitted to the

IPT a statement revealing that every UK citizen who uses services including Google, Facebook, Twitter and YouTube can be monitored by the security agencies, on the basis that these were deemed to be “external communications.” This was also the case for emails to or from non-British citizens abroad.

Privacy International continued, “Other previously secret ‘arrangements’ revealed during the case showed Britain’s intelligence services can request or receive access to bulk data from foreign agencies like the NSA without a warrant, whenever it would “not be technically feasible” for the government to obtain it themselves.

Carly Nyst, Legal Director at Privacy International, said, “The proceedings forced the government to disclose secret policies governing how foreign intelligence agencies, including the NSA, share information with GCHQ.”

Nyst added, “The IPT must find that secret law is not law, and should at the very least rule that all UK access to PRISM was unlawful prior to today.”

The organisation said that as the IPT decision was based on “hitherto secret government policies which were only made clear as a result of the IPT claim,” they were seeking “a declaration from the Tribunal that GCHQ’s actions prior to acknowledgment of these policies were unlawful.” It reported that this application will be decided by the IPT within weeks.

Privacy International and Bytes for All are also appealing the IPT’s ruling to the European Court of Human Rights.



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact