PRIVACY INTERNATIONAL

Report

Human Rights Issues with the draft Communications Data Bill

July 2012

Report

Human Rights Issues with the draft Communications Data Bill
July 2012

PRIVACY INTERNATIONAL

www.privacyinternational.org

Summary

This report was submitted to the Joint Committee on Human Rights. Under the current version of the draft Communications Data Bill, records of every person or entity with whom any given individual has communicated electronically would be collected continuously and stored for one year. These records would include the time of the communication and the location from which it originated.

The Communications Data Bill raises a number of concerns with regards to the right to privacy under Article 8 of the Human Rights Act. There are also concerns about the right to free expression under Article 10 and the right to freedom of assembly and association under Article 11 due to the potential chilling effect of the 'menace of surveillance' (Klass v Germany), but as these apply more generally to the broader domain of communications surveillance in the UK, we have restricted our comments to Article 8 issues for the purposes of this response.

Many thanks to Covington and Burling who assisted with the preparation of this submission.

How Article 8 is engaged

The European Court of Human Rights (ECtHR) held in Amann v Switzerland (2000) that "the storage by a public authority of information relating to an individual's private life amounts to interference within the meaning of Article 8" and that the "subsequent use of the stored information has no bearing on that finding". In Amann, the European Court of Human Rights found Article 8 applicable when state security services kept records indicating that the applicant was a contact of the Soviet Embassy, after intercepting a telephone call from the Embassy to the applicant. The Court noted that storage of the information on an index card alone was sufficient to constitute an interference in private life. Similarly, in Rotaru v Romania (2000) the Court found that the storing by the security services of information about the applicant's activities while a university student constituted an interference with his Article 8 rights. Collecting and storing private information is therefore an activity that will always engage Article 8; whether or not the state ultimately uses that information against an individual is irrelevant.

The European Court of Human Rights has repeatedly found the recording of numbers dialed from conventional telephones to constitute an interference with private life. In an earlier technological era, the Court pointed out that information about who called who (traffic data) was an important element of telephone communications information. Indeed, the information at issue in Amann – that the applicant was a contact of the Soviet Embassy – could have been inferred just as easily from traffic data as it was from interception of the content of the communication. Recent technological advances have blurred the distinction between traffic data and content still further. Mobile phone companies are now able to record the exact location from which a call is made, internet service providers (ISPs) can track every web page visited by their users, and the address lines of e-mails provide a wealth of data about the circles of people with which an individual interacts. All of this information, and more, may be stored under the terms of the draft Bill.

ECtHR decisions over the years have acknowledged that Member States must have the capabilities to effectively counter threats such as espionage and terrorism, and that this will sometimes include undertaking secret surveillance. However, the Court has also held that the state "may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate" due to the danger of such laws undermining or even destroying democracy in the name of defending it, see Klass.

Why we believe the draft Bill may be in contravention of Article 8

The Human Rights Act 1998 states that there shall be no interference with the right to privacy as protected by Article 8, "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

In accordance with the law:
In Malone v UK (1984) the Court ruled that the expression "in accordance with the law" means not only that any interference with the right to privacy must have some basis in the law of the country concerned, but also, over and above compliance with domestic law, it requires that domestic law itself be compatible with the rule of law. There is therefore an implied requirement for a measure of legal protection in domestic law against arbitrary interferences by public authorities. The Court accepted that the law does not have to be such that an individual should be able to foresee when his communications are likely to be intercepted so that he can adapt his conduct accordingly. However, the law must be sufficiently clear in its terms to give citizens in general an adequate indication as to the circumstances in which, and the conditions on which, public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. Furthermore, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the substantive law governing communications surveillance and interception itself, as opposed to accompanying administrative practice, must indicate the scope and manner of exercise of any such discretion with sufficient clarity, having regard to the legitimate aim of the measure in question, in order to give the individual adequate protection against arbitrary interference.

In Kruslin v France (1990), the Court found that a law authorising telephone tapping lacked the requisite foreseeability because it nowhere defined the categories of people liable to have their telephones tapped or the nature of the offences which might justify such surveillance. In Amann, the Court reached the same conclusion with regard to a decree permitting the police to conduct surveillance, because the decree gave no indication of the persons subject to surveillance or the circumstances in which it could be ordered. Blanket data retention also offends the principle of foreseeability because it makes no distinction for relationships that the state recognises as sufficiently special to warrant a degree of protection. In

Kopp v Switzerland (1998) the Court observed that a law authorising interception of telephone calls would in certain circumstances contradict other provisions of Swiss law according protection to confidential attorney-client communications. The Court found that the telephone-tapping law failed to meet the standard of foreseeability, because it provided no guidance on how authorities should distinguish between protected and unprotected attorney-client communications.

Necessary in a democratic society:
In Foxley v UK (2001), the Court ruled that Article 8 was violated by the unnecessary and disproportionate interception of correspondence, which included correspondence between the applicant and his solicitors. The legal basis for the interception was the Insolvency Act 1986, under which a court ordered the redirection of the applicant's mail to a trustee in bankruptcy. However, the intercepts continued after the expiry of the court order; this was unjustified and violated Article 8. The Court stated that "the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued". In S and Marper v UK (2008), the Court held that the retention of the DNA profiles of suspects after they are acquitted or the charges against them are dropped is a violation of Article 8, and commented on the "blanket and indiscriminate nature of the power of retention in England and Wales".

- The draft Communications Data Bill as it stands creates a system of blanket collection and retention of data that fails to distinguish between different classes of people. It would be even more pernicious than the overly vague legislation in question in Kruslin and Amman – whereas these laws left citizens vulnerable to the possibility of surveillance, the draft Bill would subject citizens to the near certainty of ongoing and unremitting interference in their private lives.

- Directive 2006/24/EC (the Data Retention Directive) already requires Member States to retain data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks for between six months and two years. The draft Communications Data Bill would dramatically expand this regime by requiring telecommunications companies and ISPs to collect new types of information about their users that they do not require for business purposes. It is also worth noting that the constitutional courts in Romania are blocking the implementation of the directive on the basis that it conflicts with the citizen's right to secrecy of correspondence enshrined in the Romanian constitution and heavily implied in Article 8, Bulgaria's Supreme Administrative Court ruled in 2008 that the directive did not comply with the national constitution or the European Convention on Human Rights, and the European Court of Justice is currently reviewing a case against the directive brought by Digital Rights Ireland.

- The nature of this draft Bill is such that Parliament cannot foresee how it will be applied due to the vast scope of executive discretion with regards to future

expansion of the surveillance regime it grants. The legislature is therefore being asked to sign off on piece of legislation that will allow the Home Secretary to order companies to implement new measures to collect new forms of information about an undefined number of people, for an undefined purpose, for an extended period of time.

- There is very little international precedent for this kind of legislation, and as such the United Kingdom would be alone in the democratic world in mandating this kind of communications data retention. The technology that will be used is only currently deployed by Kazakhstan, China and Iran. It is difficult to see how such measures could therefore be necessary in a democratic society.
- The police will be able to self-authorise access to the retained communications data; the self-authorising standard was created by the Regulation of Investigatory Powers Act (RIPA) and remains one of the lowest standards internationally.
- Alternative means of gaining access to much of this information already exist under RIPA, under which the Secretary of State authorises interception of communications. These targeted surveillance measures provide a stronger safeguard, while ensuring access to much of the data necessary for criminal investigations. This proposed regime downgrades existing standards for access to these data types.

Opportunities to protect human rights

The revisiting of the regulation of policing methods with regards to new surveillance technologies could have resulted, and could still result, in greater clarity and protections. For the past two years, Privacy International has been researching the global surveillance industry, focusing on technologies that are developed in countries like the UK, the US and Germany and sold to undemocratic countries in the Middle East and Africa. However, we have also become aware that many of these technologies are being used in the UK. It is difficult to see how existing legal regimes can be applied to the use of these technologies by the police and other public authorities. The tools now available allow the user to:

- remotely access an individual's computer or mobile device using hacking techniques in order to covertly gain complete control of the system, including the ability to remotely switch on the computer/device's camera and microphone
- identify all mobile phones, and subsequently their owners, in a given radius (up to several hundred metres) through the use of 'IMSI-catchers'
- establish false mobile phone towers in order to intercept all communications in a given area, e.g. allowing the police to passively monitor all communications at a public event
- infiltrate and monitor social networks

The JCHR would be perfectly suited to begin the discussion on this, and this legislative window opened by the Draft Communications Bill is ideal since it is re-evaluating the powers under the Regulation of Investigatory Powers Act.