Scottish Business Resilience Centre
Creating a secure Scotland for business to flourish in

22 Dec 2015

Encryption and the IP Bill

Is the government planning to end the use of encryption after all?

The UK Government published a draft Bill at the start of November entitled the Investigatory Powers Bill (IP Bill). This is the Government's second attempt to cure the perceived problem created when the EU struck down its own Directive in April 2014 on the basis that the surveillance permitted was no longer justified in light of an individual's right to privacy, family life and the protection of their personal data.

Under the Directive communication companies were required to retain data for between 6 months to 2 years from landlines, computers, fax machines and mobile phones.

The first attempt to cure this perceived problem was through the Data Retention and Investigatory Powers Act which was given a total of three days scrutiny by Parliament before it became law in July 2014. It was successfully challenged earlier this year by two MPs (David Davies and Tom Watson) represented by Liberty when the High Court ruled that certain sections were unlawful essentially because the correct balance between privacy and surveillance had not been struck.

The IP Bill obliges communication companies to hold a year's worth of communications data which will include details of the services, websites and data sources individuals connect to when they go online. It does not include the detail of what individuals did within each service.

The oversight is to come from a new body called the "investigatory powers commission" led by senior judges who will act as a "double lock" on interception warrants. When a minister signs off an application to monitor communications, the operation won't begin until the commissioners have also agreed. This has been criticised by some commentators as a rubber stamping exercise rather than proper scrutiny.

There was also concern prior to the draft Bill being published that encryption was going to be outlawed. Theresa May indicated that was not going to happen but some communications companies have expressed concerns about how the Bill might be interpreted in the future.

Section 189 of the bill, titled "Maintenance of technical capability", allows the Secretary of State to issue orders to companies "relating to the removal of electronic protection applied … to any communications or data" and the only limit on this power is a requirement that they consult with an advisory board beforehand, and that any specific obligation must be "reasonable" and "practicable".

The concern relates to companies who provide "end-to-end" encryption allowing a message sent between two individuals to be protected in such a way that no one other than the sender and recipient can read it. Even the company that facilitates the communication cannot decipher the messages this way. For communications with end-to-end encryption enabled, bulk surveillance is difficult, since only the metadata around the communications can be read without the encryption key.

Under the IP Bill as currently drafted it appears that the UK government could issue a technical capability order requiring the communications firms to disable their end-to-end encryption, or replace it with a weaker form of encryption, which would leave the communications facilitator able to read messages sent using its service. The only defence the firms would have would be to argue such an order is not "reasonable". We intend to keep a close eye on the progress of the Bill and in particular the implications for encryption.