Why tech companies are really worried about the snooper's charter

Alex Hern

Tuesday 10 November 2015 05.04 EST

Technology firms could be forced into a no-win situation if the UK government's investigatory powers bill passes without substantial changes from its current draft form.

The legislation includes a number of clauses which are scaring technology firms. Under the proposals they can be required to provide assistance to the government to hack their own users; they can be mandated to open their networks up to bulk interception of data; and they can be required to modify their technologies to make the interception of data easier, even to the extent of removing "electronic protections" applied to them.

That last requirement is what's most concerning for tech companies, since it seems to imply that the government may start asking them to rewrite their apps to remove encryption – or, at least, to alter the way the cryptosystems work so that the technology firms themselves can snoop on their customers' messages.

It's prompted a rare intervention in British politics from Apple chief executive Tim Cook, who said on Monday that the company "believes very strongly in end to end encryption".

Cook added that "if you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things. It's the good people. The other people know where to go".

But the government was adamant in the lead-up to the bill's introduction that it wouldn't be attacking encryption, so why are the tech companies now concerned? The reason seems to be a couple of sleights-of-hand.

The first is that the requirement that telecommunications operators weaken their own encryption if asked to do so – known as a "technical capability order" – is already in British law in the Regulation of Investigatory Powers Act 2000. The government has thus positioned the clause in the investigatory powers bill as a mere continuation of that power, albeit one written into legislation for the first time.

But that's disingenuous. The RIPA power, crucially, works with a very different definition of "telecommunications operator". Under RIPA you have to provide telecommunications services, meaning that internet service providers, mobile carriers, and the like are covered, but tech companies aren't. RIPA was drafted four years before the launch of Gmail, let alone messaging applications such as iMessage and WhatsApp.

The tech companies warn that the new bill has a wider definition of telecommunications operator which covers companies like Apple and Facebook, as well as the old ISPs. Amongst the carefully redrafted legislation, for instance, the phrase "public telecommunications service" has been replaced with "telecommunications service".

The second issue is how the government has managed its messaging on encyption.

In the House of Lords, Baroness Shields was clear: "The government recognise the essential role that strong

encryption plays in enabling the protection of sensitive personal data and securing online communications and transactions. The government do not advocate or require the provision of a back-door key or support arbitrarily weakening the security of internet applications and services in such a way".

But that's not the whole picture. While the government is fine with encryption between an individual and a company, which can be hit with a warrant, it isn't so happy about encryption between two individuals which can't be decrypted by a middleman.

Hence the technical capability orders. If a company is offering this sort of encryption – known as "end-to-end" encryption, because the message is encrypted from one endpoint to the other – the government reserves the right to order that company to rebuild its systems to enable eavesdropping.

Those orders can apply to any company, even one based in a country other than the UK, and can mandate changes to equipment in or out of Britain. Ultimately, if the order isn't carried out, the penalties rise to "fine and imprisonment" if the court sees proper.

So what will happen if the government does decide to mandate a technology company to remove its end-to-end encryption?

Initially, a long and ugly legal battle. Whichever company decides to go to bat first would be arguing on two fronts: firstly, trying to claim that the law doesn't apply to them in the first place, by focusing on the contested definition of telecommunications service provider; secondly by trying to argue that the request doesn't fulfil the terms of the law anyway.

One defence they have is that the law limits requests to those that are "reasonably practicable". Whether a tech company considers the request to remove end-to-end encryption "reasonably practicable" depends on who you speak to: one tech insider told me that it would be an easy victory, because if the users hold the encryption keys, there's no way it can be reasonable to demand the company breaks encryption they can't decrypt; but another insider was less hopeful that such an argument would be victorious.

If the rebuttals fail, then any tech company would be faced with a nasty proposition: either a very public climbdown from previous promises to offer end-to-end encryption, or a partial or total withdrawal of encrypted services in Britain – or the prospect of the company's most senior executives facing fines or imprisonment.

Popular services that use end-to-end encryption include Apple's messaging service, iMessage, and the Facebook-owned WhatsApp. But other tools, from PGP to Tor, offer the same security in a package that is nearly impossible for the government to crack down on. As a result, the services you and I use could be caught in the crossfire by an investigatory powers bill that will do nothing to stop the bad guys – whoever they may be.

"