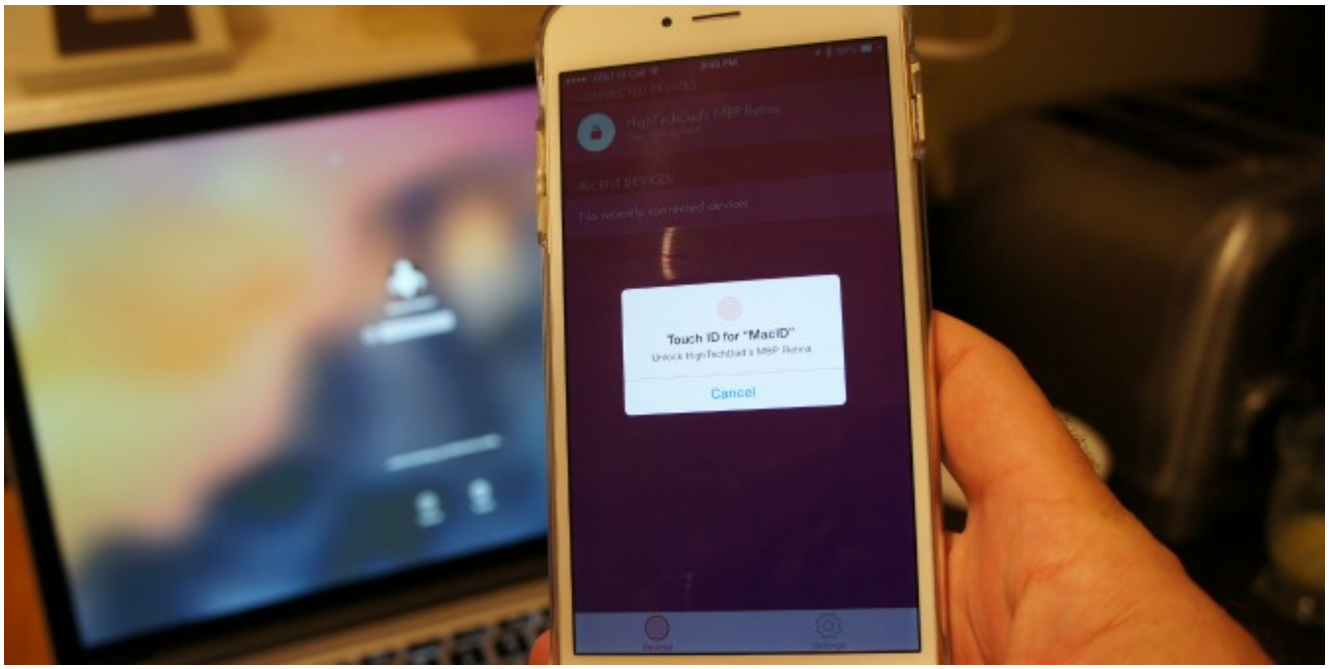
# You can’t deny message encryption to some individuals without denying it to all

blogs.lse.ac.uk/businessreview/2016/03/08/you-cant-deny-encryption-to-some-individuals-without-denying-it-to-all/

3/8/2016




Some of the more dramatic headlines surrounding the new surveillance law, the Investigatory Powers Bill (‘IP Bill’) which is currently making its way through parliament, have surrounded its impact on popular messaging apps such as WhatsApp, Apple’s iMessage and many more. Will the IP Bill ‘ban’ what is generally known as ‘end-to-end encryption’, where the content of a message can only be read by those at either ‘end’ and not by those in the middle, including the provider of the app, such as WhatsApp or Apple themselves? Will it force the providers of apps to build in ‘back doors’ to allow the authorities access to the messages?

**Parliamentary Committees wanting clarity**

The answers to both of those questions, unfortunately, are far from clear. It wasn’t clear in the first draft of the IP Bill in November 2015 – so unclear that all three of the parliamentary committees that looked at the bill asked for further clarity. The Science and Technology Committee said in its report that:

“There is some confusion about how the draft Bill would affect end-to-end encrypted communications, where decryption might not be possible by a communications provider that had not added the original encryption.”

The Intelligence and Security Committee said in its report that:

“Some CSPs have expressed serious concern as to this seemingly open-ended and unconstrained power, suggesting that this may lead to banning end-to-end encryption. The Home Office must ensure that the legislation provides clarity as to the nature and scale of these obligations.”

The specially convened Joint Parliamentary Committee on the Investigatory Powers Bill said in its report that:

“The Government still needs to make explicit on the face of the Bill that communication service providers (CSPs) offering end-to-end encrypted communication or other un-decryptable communication services will not be expected

to provide decrypted copies of those communications if it is not practicable for them to do so."

However, when the new draft of the Bill came out in March, the changes did not seem to be sufficient. Though the Home Office claimed it was creating clarity, few readers of the Bill, the codes of practice that accompanied it and even the special 'factsheet' on encryption' that followed a few days later, felt that there was very real change – or sufficient clarity. The Home Office went some way towards what was recommended, but left enough vagueness to cause considerable concern.

**Technical Capability Notices**

The possible requirement to remove or bypass encryption is covered in what are termed 'Technical Capability Notices. The relevant part of the draft bill says:

"The Secretary of State may give a relevant operator a notice (a "technical capability notice")—

(a) imposing on the relevant operator any applicable obligations specified in the notice, and

(b) requiring the person to take all the steps specified in the notice for the purpose of complying with those obligations."

These obligations could include:

"obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data;"

On the face of it, this looks as though it might require the 'relevant operator' to remove encryption – something which would fundamentally undermine end-to-end encryption. Putting in 'by or on behalf of' goes part way to meeting the Science and Technology Committee objection – but what 'on behalf of' means is debatable. There are further caveats built into the Bill, caveats which the Home Office seems to think cover the problems. The Secretary of State must take into account whether the notice is 'technically feasible' and the obligations imposed must be 'practicable'. It is in these two terms that the real problem lies. Both are vague and subjective – and leave any operator of a messaging service in significant doubt as to what they might be asked to do.

There are further problems for the messaging services. If they are served with such a notice, they cannot disclose that fact without the permission of the Secretary of State – so amongst other things they cannot find out whether other operators have attempted to comply or not. Notices can be applied whether the operator is in the UK or overseas – but enforcement overseas could be very difficult, leaving the UK technology industry in a more vulnerable position.

**Underlying problems**

The underlying problems may be even more significant. The technology industry worldwide is moving towards the idea of strong encryption that the providers themselves cannot – and will not attempt to – break. The current conflict between Apple and the FBI over the protection applied to the iPhone of the San Bernadino shooter has shown that Apple will fight very hard to keep that protection – and most of the technology industry has come out very strongly on Apple's side of the battle.

There are good reasons for this – and fundamental problems with the approach taken by the Home Office in the Investigatory Powers Bill as a result. As their Factsheet on Encryption puts it, with reference to 'terrorists and paedophiles':

"It is absolutely crucial that there is not a guaranteed safe space online in which these individuals can communicate, beyond the reach of our law enforcement and security and intelligence agencies."

The problem is, if this ‘guaranteed safe space’ is denied to *these* individuals, then it is denied to *all* individuals. End-to-end encryption is essentially intended to provide exactly this guaranteed safe space to all individuals. If the Home Office, therefore, really intends to deny this, then no matter what it says to the contrary, then it *does* seek to ban or fundamentally undermine end-to-end encryption.

That, at present, appears to be what the Investigatory Powers Bill says. Through Technical Capability Notices, it allows the Secretary of State to demand that the encryption built in to a messaging app be broken by the provider of that app. Arguments about whether this is ‘practicable’ and ‘technically feasible’ do not provide sufficient protection for the app providers to feel secure: the pressure to ‘find a way’ could well become intolerable.

In the end, however, it is likely that the Home Office is fighting a losing battle. Theresa May is setting herself up, Canute-like, to try to hold back a tide towards strong encryption that is likely to be irresistible. It may be a long time, however, before she and others in similar positions are willing to accept this.

♣♣♣

*Notes:*

- *This post gives the views of its author, not the position of LSE Business Review or the London School of Economics.*
- Featured image credit: Intel Free Press CC-BY-SA-2.0

---

**Paul Bernal** is a Lecturer in Information Technology, Intellectual Property and Media Law at UEA Law School. His PhD on internet privacy was completed at the LSE in 2012, and he is the author of Internet Privacy Rights: Rights to Protect Autonomy, published by Cambridge University Press in 2014.