TCN NOTICES CONSULTATION

Response to Consultation on revised notices regimes in the Investigatory Powers Act 2016

July 2023

Introduction

ORG would like to express concern regarding the proposed changes, which seem to be squarely aimed at reducing the possibility of the introduction of encryption to protect user data from unwanted access.

The Home Office appears to regard encryption, especially “end to end encryption” (E2EE), where a service provider is unable to see the contents of communications they facilitate, as a threat to its capabilities, and by extension, to national security. It appears to be seeking to extend its powers to prevent E2EE from being used at scale, despite its benefits to users and vendors.

E2EE is a significant protection against everyday criminality, abuse and intrusion. E2EE protects vendors from being a vector for potentially massive data loss, with often traumatic consequences, where the data is especially personal. The increase of encryption should be seen as a benefit, as has been highlighted by the former head of the NCSC.

Where encryption has been introduced or is sought to be introduced, it is typically because of a threat to individuals’ data that would have high impacts if accessed by criminals; or else because abuse or interference in that data is already routinely taking place, but is difficult to enforce against.

In either case, limiting the roll-out of encryption because of law enforcement considerations risks enabling criminal or unlawful behaviour, and places large numbers of users at risk, in order for the Home Office to have the easiest means to address questions of lawful access, which can however usually be addressed by other means.

Large numbers of UK professionals – doctors, lawyers, accountants, management consultants, IT experts – deal in personal data which they are required, under Data Protection legislation, to exchange securely with others. They exchange information via encrypted services and encrypted file attachments. The current proposals undermine these routes and with significant implications for the UK's service

economy. The services industry amounts to 79% of UK GDP.[1]

While the government may have particular reasons to seek access to data and systems in certain limited circumstances, it should neither assume that all data should be easily accessible nor seek legal regimes to ensure that data is kept easily accessible.

We reiterate that encryption does not prevent lawful access per se. It may require law enforcement to covertly access a device, or to seize it and demand passwords; however these approaches are likely to be more proportionate than simply preventing security measures from evolving for the population at large.

Finally, it is worth noticing that the consultation does not provide meaningful explanation as to what changes the government are planning to introduce and why. In particular, the consultation lacks details concerning safeguards and conditions that would apply to the issuing of these notices under the (unclear) revised terms. These changes also affect respondents' ability to comment on the effectiveness of the Judicial Commissioner's oversight under the new regime, which will depend on the breadth of discretion being given to the Secretary of State for the issuing of these notices. The overall approach to this consultation appears quite dubious and wholly inadequate and raises more questions about what is being omitted rather than about what is being proposed.

Proposed objectives of the changes

The objectives outlines are concerning especially when taken together. Under *Objective 1 – Strengthening the notice review process,* the consultation states that:

> "When giving a notice for the first time the Secretary of State has a statutory obligation to engage in a consultation period with the relevant operator. … during a review period the operator is not required to comply with the notice, so far as referred, until the Secretary of State has concluded the review …
>
> Where an operator is seeking to make changes to their system that would have a detrimental effect on a current lawful access capability, this could create a capability gap during the review period, which is an issue we believe should be addressed.
>
> This could be done through a general requirement to maintain the status quo through this period, ensuring that our lawful access to data is maintained."

Likewise, *Objective 2 – Timely and informative responses* asks that

1 House of Commons Library 14/07/2023

> "there should be an obligation placed on the operators to cooperate with the consultation process before the decision to give a notice is made, and with any subsequent review process, and to provide relevant information as necessary and within a reasonable time."

These objectives appears to be designed to impose a "freeze" on changes to the service while consultations are taking place. The intention appears to be to stop improvements to user security from being rolled out.

While this objective may appear to be reasonable, it would allow the Home Office to prevent secure services from launching in the UK, even where they are rolled out elsewhere. This provision would allow the Home Office to place itself in a position of power over the provider as soon as it hears about the possibility of data being less accessible than it is currently. This situation would take place without reference to an independent authority to assess the rationale or proportionality. Such a move might not be proportionate, for instance, if the security technology had already been introduced safely and with demonstrable benefits to users in other parts of the world.

We understand that the Home Office has already intervened in the use of encrypted technologies that are widespread in other parts of the globe, but are either delayed or less available in the UK. The change in powers suggested would make it easier for the Home Office to routinely intervene to delay roll out of security improvements, making the UK a far less attractive place for digital businesses as well as less safe for its citizens.

At present, we believe that some companies have complied with Home Office requests to negotiate over security changes. The Home Office is able to request that the company comes to an agreement with them about a suitable way forward, and not to implement any changes until this is done, under threat of a Technical Capability Notice should they proceed without agreement. Since agreement is often not possible without compromising the premise of encrypted communications, the company is left unable to conclude its negotiations. This conundrum nevertheless suits the Home Office, as preventing the proposed security improvements is its goal.

With the proposed power, should a company call the Home Office's bluff, and say that in fact they will proceed with their security improvements, and that they might simply withdraw from the UK market should they be issued with a TCN, then the Home Office could simply start the TCN process, in order to freeze the technology for UK users. The company would find it much harder to conclude the process satisfactorily.

Under *Objective 4 – notification requirements,* the Home Office proposes:

> "to make changes that would support cooperation between government and industry by setting clear expectations about the circumstances in which operators might be expected to notify the Secretary of State of planned changes to their service that could have a negative impact on investigatory powers and, where necessary, mandating notification of planned changes. …
>
> we propose to introduce a requirement for the Secretary of State to consider the necessity and proportionality of imposing a requirement to notify, including taking into account the impact on the business or businesses to whom it will apply as well as the likely benefit of early notification. This would avoid placing burden on those telecommunications operators whose data is of minimal operational importance. …
>
> Additionally, we intend to develop a series of thresholds that would also trigger the notification requirement, for example, if a technical change could substantively impact existing IPA capabilities or the availability of communications and communications related data for a certain number of users or a certain percentage of the market. We welcome comments from respondents on this approach, including potential thresholds."

It is unclear whether the notification requirement would exist without a TCN being in place, or whether one might be issued to a company to provide broad access to data without any specific changes being required, and then be used to limit any changes that would improve user security in the future. The requirement appears to be aimed at ensuring that any large digital provider would be obliged to explain if any of its services might be made more secure, in order that the Home Office be able to prevent security measures from being put in place.

Combined with the first three objectives, this requirement forms a strategy whereby the Home Office seeks to know about any possible secure service being introduced, and then intervenes to stop it from being rolled out.

Compromising technology and companies

A further result of this strategy is that companies may be asked to lie about the security of their products, after compromising them to introduce 'back doors', or may be asked to provide services they believe are sub standard and produce risks to their users. There are reputational issues to making such compromises, should compromises become apparent, and the UK will be known as a sub-standard place for digital business. This strategy is unreasonable, and may lead to companies leaving the

UK market. At best, it may mean that improved security available to people elsewhere is specifically unavailable in the UK.

Extraterritoriality

It must also be made clear that the UK cannot and should not purport to be able to "freeze" the development and deployment of products outside of the UK. Other countries are governed by the rule of law and have their own, potentially conflicting, requirements and allowances. The UK should not purport to be able to veto the development and deployment of security technologies that could be beneficial to millions of users outside of the UK.

Proportionality of the Home Office strategy

It is unclear that it is possible to make the Home Office's overall strategy proportionate, if the intended outcome is to limit the introduction of E2EE or other security technologies and thereby reduce the security of millions of users.

As the strategy relies on coercive powers, to start processes which would stall the deployment of security technologies with the intention of preventing or compromising their introduction, the proportionality test would need to be made both at the start of the process, and particularly at the level of the Home Office's overall strategy of preventing the use of these security technologies.

Unfortunately, as the use of these powers in practice seems to be through the informal use of the potential threat of a TCN, to dissuade companies from taking steps the Home Office does not like, the use of these powers to prevent the deployment of E2EE and technology security improvements is in practice often not subject to any proportionality test whatsoever.

Finally, the government propose "to introduce a requirement for the Secretary of State to consider the necessity and proportionality of imposing a requirement to notify." While the wording of this proposal appears rather vague, it is reasonable to assume that the government intends to introduce a requirement in legislation to "have regard to" necessity and proportionality. This change, however, would represent a soft requirement that fails to provide a legally binding safeguard—indeed, the Secretary of State may even decide to breach proportional and necessity when issuing a notice, insofar as it had "regard" of it. As such, this change would fail to ensure the proportionality of the regime and would instead create an arbitrary and unaccountable power in the hands of the Secretary of State.

Minimum change needed

At a minimum, if companies are to be subject to a coercion, such as temporarily making no changes to their technologies as set out in Objective 2 and 3, or notifying the government of intentions to change technologies, as set out in Objective 4, then these requests should be subject to the ‘double lock’, and be tested for proportionality.

An alternative strategy

The Home Office should cease being concerned about the increase of the use of encrypted technology, but rather should see it as a benefit against routine criminals. It should assess the specific alternative methods of access it has available. It should improve the investigative abilities of law enforcement.