Encryption and government regulation: what happens now?

Kevin Smith, Vodafone R&D| IAB MaRNEW workshop, September 2015

Abstract

End-to-end encrypted traffic now accounts for ~45% of the total transited by mobile networks[1], which impedes the ability for networks to carry out content filters imposed by government regulation. This paper outlines three categories of filters, the impact of encryption on each, and concludes that governments are likely to explore other means to enforce regulatory requirements, possibly including endpoints. The paper also notes the impact of encrypted 3rd party communication services on Lawful Intercept regulation. A discussion of censorship or abuse of this blocking regulation, whilst valid, is out of scope; rather the paper aims to encourage discussion on technical reactions to any regulatory changes.

Government regulation of mobile network operators

Content blocking

Mobile network operators are regulated by government, as a condition of their operating licences and other legislation. Refusal to comply with a country's laws is not an option for a network operator: non-compliance with a lawful demand for assistance can result in removal of the operation licence, and operator employees who live and work in the country concerned may also be at risk of harm or criminal sanctions, including imprisonment.

As regards user access to Internet content, these regulations tend to fall into three categories: court order blocks, adult content controls, and Internet Watch Foundation blocks on child sexual abuse materials. This paper uses the United Kingdom as an example, but recognises there will be differences in regulation and implementation across territories. Filters apply on addresses, not on the content itself.

A **'Court order' block** has (as the name suggests) gone through judicial process to mandate the blocking of URL(s) by network operators. Claimants in such cases are typically rights-holders (e.g. media publishers wishing to stem the flow of free access to copyright content) or governments preventing access to offshore gambling sites. In some territories the Interpol 'worst of the worst'[2] list may also be implemented by Court Order. The UK government has no ability to directly request to block a URL/IP address outside of this framework [3], unless the network is a host of the content.

Adult filters act on age-inappropriate content (violence, sex etc.). Possibly unique to the UK is that a mobile connection is assumed to be a 'child' by default, and must be verified as 'adult' in order to change that default. The enforcement of these filters is effectively mandatory by UK operators.

Internet Watch Foundation is a non-governmental organization providing an 'opt in' service to block access to child sexual abuse materials [4]. This speed at which Websites hosting such content change URLs means that it is not feasible to rely on the Court Order process for blocking. Implementation is via

a ‘black box’ filter hosted within the mobile network – the network operator has no visibility of the URLs stored within.

Technical implementation of blocks

A filtering function is placed into the 3GPP core network of the operator, between the Internet interface and the air interface. This function can filter IP addresses/ranges, domains including wildcards, and URLs including filtering on path segments. Court Order blocks are typically per domain, adult content filters can be per domain or URL with path segments. Internet Watch Foundation and Interpol lists are not available for analysis.

The impact of encryption on this regulation

Unencrypted Internet requests reveal the IP 5-tuple and URL to the mobile network. HTTPS encrypted traffic will hide the path segment of a URL, but will reveal the server name indication in most cases today, indicating the domain. So the impact on the blocking categories is:

- Court order blocks: may still be implemented where SNI is provided
- Adult content filters: may still be implemented where SNI is provided, but the key challenge is for sites hosting both universal and adult content. Examples include tumblr and Twitter – the filter would apply to the full URL path, but that is hidden from the network in HTTPS.
- IWF/Interpol lists: under investigation, due to list contents being unavailable to operators.

So ‘URL path’ based filtering is no longer possible, but domain based filtering is, mainly impacting adult content filters. However: where the domain is also obscured, for example as an encrypted extension in TLS 1.3, then there could be a significant impact on the network operators’ capability to implement regulations.

Lawful intercept of personal communications

A law enforcement agency (LEA) will be granted access to personal communications following application of an intercept warrant from senior government ministers [3]. Where the network operator is the communication service provider, for example for a 3GPP voice call, then the communication is expected to be made available in its unencrypted form to the LEA.

Impact of encryption

Where the network operator is not the provider of an encrypted communication service, but rather acting as a ‘mere conduit’, then it is understood that the network cannot provide a cleartext of the communication. This applies to encrypted messaging apps or Web services.

Conclusion: predicted reaction of regulators to ubiquitous encryption

This has two aspects: the application of filters, and lawful access to personal communications.

Content filters

Encryption chiefly affects the ability to filter against URL path, and hence adult content filters. Should future encryption protocols (e.g. TLS 1.3) also hide the domain from the network, then the government

will need to consider other means to enforce court order blocks. This may include blocks against IP addresses only, with the caveat that these may not be static for a given service.

Net Neutrality

We must also consider Net Neutrality when discussing filters. The UK government may interpret EU Net Neutrality directives as indicating 'no filtering', and legislate accordingly. Note that this decision is not likely to affect Court Order blocks, which are also legislation; however this may effect adult content filtering, for example enforcing an explicit opt-in to filtering rather than today's opt-out. It would also affect filtering against IWF and Interpol lists, which may need to move into legislation in order to be implemented. The impact in terms of encryption is therefore that the need to account for content filtering in general may diminish.

Lawful intercept

This appears to be the focus for UK government, namely lawful intercept of peer-to-peer encrypted communication services, where that service is not managed by a regulated operator [5]. A reaction to this has been posted by respected academics and industry experts [6], which warns against any backdoors being introduced to security mechanisms to allow governments access, since that is likely to introduce weaknesses. One approach by government may be to regulate endpoints, such as Internet clients (apps/ An *impasse* in this argument may result in radical legislation, such as blocking encrypted messaging services outright, which would be detrimental to law-abiding users and likely to result in an 'arms race' of VPN, proxy and TOR services being used to bypass the blocks. It

Request for comments

The paper asks that the IAB/IETF consider any technical options for lawful intercept and content filtering in an encrypted Internet, with the aim of providing a Best Current Practice document that supports the complex (and competing) requirements of privacy, security and regulation.

References

[1] GSMA Web Working Group anonymized survey, 2015

[2] http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Criteria-for-inclusion-in-the-Worst-of-list

[3] http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/law_enforcement_disclosure_report_2015_update.pdf

[4] https://www.iwf.org.uk/members/member-policies/url-list/blocking-faqs

[5] http://www.theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws

[6] 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', Abelson et al., http://dspace.mit.edu/handle/1721.1/97690 , July 2015