Openforum europe

open, competitive choice for IT users

Submission from OpenForum Europe to the Science and Technology Committee in response to the Committee's enquiry into the technology aspects of the draft Investigatory Powers Bill [1]

Submitted on 27 November 2015

About OpenForum Europe

OpenForum Europe (OFE)[2] is a not-for-profit industry organisation which was originally launched in 2002 to accelerate and broaden the use of Open Source Software (OSS) among businesses, consumers and governments. Since then, the role of OFE has evolved, and we now devote much of our time to explaining the merits of openness in computing to politicians and legislators across Europe, as part of a vision to facilitate open, competitive choice for IT users.

In the United Kingdom, OFE has launched a formal OFE UK 'Chapter', the Community for Open Interoperability Standards (or COIS), firmly endorsing the UK Cabinet Office's Open Standards Principles, and with the goal of allowing wider and easier interchange between community volunteers and supporters and the public sector.

OFE is supported by major IT suppliers, as well as a number of national partners representing SMEs from across Europe. Views expressed by OFE, however, do not necessarily reflect those held by all its partners and supporters. For more information about OFE, please visit our website.

Introduction

OFE welcomes the opportunity to comment to the Committee on the technology aspects of the Draft Investigatory Powers Bill which was published early in November. OFE understands and acknowledges the need to review and consider possible adaptations to the UK's existing surveillance legislation, particularly in light of increasing and evolving threats. At the same time, any such review process should include consideration of the impact of the Draft Bill in terms of the

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

2 OFE Limited, a private company with liability limited by guarantee; registered in England and Wales with number 05493935; registered office: 1 Blunt Road, South Croydon, Surrey CR2 7PA, UK

economic consequences, respect for personal privacy and whether any such changes could have consequences for securing our networks and preventing cybercrime and other harm. OFE's contribution at this stage will focus on the obligations that would be imposed under the Draft Bill on communications service providers (or CSPs).

Encryption makes us more secure, not less

People all around the world use encryption technology every day to protect themselves against harm, fraud and malicious software. This is certainly true for the consumer, where encryption is a fundamental cornerstone to secure online purchases and banking transactions, for example. It is also true for network security: encryption helps prevent attacks from organised crime, and attacks by certain nation states. Introducing "the ability to remove any encryption applied by the CSP" (otherwise known as "backdoors") generates a very real risk of making things less secure for the general public, whereas criminals will always find access to reliable encryption tools. As former US Secretary of Homeland Security, Michael Chertoff (also a former prosecutor and US Appellate Judge) succinctly said, "when you do require a duplicate key or some other form of back door, there is an increased risk and increased vulnerability. ... it does prevent you from certain kinds of encryption. So you're basically making things less secure for ordinary people."[3]

We would like to bring to the attention of the Committee a thoughtful and carefully considered recent MIT paper that examines various proposals in some depth.[4] The conclusion can be summarised as follows: (1) providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure for all; (2) building in exceptional access would substantially increase system complexity, which "is the enemy of security — every new feature can interact with others to create vulnerabilities"; and (3) exceptional access would create concentrated targets that could attract bad actors. "Our analysis applies not just to systems providing access to encrypted data but also to systems providing access directly to plaintext. For example, law enforcement has called for social networks to allow automated, rapid access to their data. A law enforcement backdoor into a social network is also a vulnerability open to attack and abuse." If security is to be reduced, even to effect a warrant, this poses more widespread problems in terms of data security and privacy. Moreover, reducing point-to-point encryption is unlikely to be a solution that could be implemented, due to the ever-changing nature of devices and locations.

3 "Michael Chertoff Makes the Case against Back Doors": July 26, 2015, found at: https://www.emptywheel.net/2015/07/26/michael-chertoff-makes-the-case-against-back-doors/.

4 "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications", Computer Science and Artificial Intelligence Laboratory Technical Report, Massachusetts Institute of Technology, July 6, 2015, found at: http://dspace.mit.edu/handle/1721.1/97690.

It should also be noted that the personal security and encryption technology adopted by the user can often impact the ability for a CSP to provide clear unencrypted data. The responsibilities of the CSP are only one part of the puzzle, and should not become the sole focal point of the new framework.

Integration and compatibility with other legal frameworks

Technology is evolving into a more and more cloud-based operation, and new devices (equipment) are being connected to the internet and the cloud at an extraordinary rate. This is compounded by the Internet of Things (IoT) and the drive to be able to obtain data from any device for analytical purposes. Security and privacy within information technology has a considerable focus in relation to IoT and Cloud, and significant effort has gone into constructing a robust standard that meets the needs of the users and the organisations using the data. It is essential that this Draft Bill not only work in harmony with other relevant Directives, but also that it respect them and their content (e.g., Directive 95/46/EC EU concerning Data Protection).

Of particular concern is the risk that a number of requirements set forth in the draft Bill as it now stands, includding the introduction of possible backdoors or mandatory reconfiguration of network capabilities, may require CSPs (and their technology providers) to put themselves in direct contravention of their obligations imposed by other relevant legal regimes, most notably at the EU level. In such cases, CSPs are likely to be caught in a "Catch-22" situation, whereby they would be forced to breach law elsewhere in order to comply with specific new requirements that are unique to the UK. As the communications in question by definition are not confined to the territory or the jurisdiction of the UK, greater legal clarity is needed to avoid such an invidious and undesirable situation arising.

OFE Limited, a private company with liability limited by guarantee
Registered in England and Wales with number 05493935
Registered office: 1 Blunt Road, South Croydon, Surrey CR2 7PA, UK