techuk.org | @techUK | #techUK

Securing a Clear Legal Framework for Investigatory Powers

October 2015

10 St Bride Street
London
EC4A 4AD

T 020 7331 2000
F 020 7331 2040
www.techuk.org

techUK | Representing the future

Contact: Talal Rajab | Programme Manager
T 020 7331 2189
E talal.rajab@techuk.org

About Us

techUK, as the trade association for the UK technology industry, represents over 850 digital technology firms. techUK's members make up many of the world's leading Communication Service Providers (CSPs)- ranging from network and infrastructure providers, domestic and small business service providers and global internet platform providers - as well as a growing number of SMEs whose activities range from telecommunications and wireless to consumer electronics and cloud based services. We also represent companies involved in the digital communications value chain, from service providers to telecoms and broadcast network providers.

Many of our members play important roles in engaging the authorities to protect the UK's national security during this period of sustained and increasing geo-political threats, and take those roles and responsibilities incredibly seriously.

Introduction

Since the start of the year three comprehensive reviews have taken place that assessed how the UK Government conducts surveillance activities; David Anderson's review into investigatory powers, Sir Nigel Sheinwald's review into international legal frameworks and jurisdiction and the Royal United Services Institute's (RUSI) independent surveillance review.

All three reviews highlighted the lack of transparency, legal clarity and effective oversight of current surveillance legislation. They concluded that government has failed to revise legislation in line with new technology, and that current legislation is unnecessarily vague and has not always operated in the public interest. User expectations of transparency and clarity have increased since 2010, and the reviews have reinforced the case for new legislation that provides clarity to companies, agencies and the public.

The upcoming Investigatory Powers Bill represents a unique opportunity to respond to recommendations made in the three reviews; strengthening the legal framework and introducing world-leading oversight of investigatory powers on the one hand and setting out a clear international framework for the lawful acquisition of data from overseas on the other.

The UK's influence and standing mean that the upcoming Bill is likely to be seen by many governments as a model to be replicated. It is therefore vital, both for UK communication service providers (CSPs) operating abroad and for the UK's benign influence on global democracy, that the Bill sets a standard that is worthy of emulation and stands up to the closest scrutiny on necessity, proportionality, transparency and oversight.

The recommendations below outline the five key issues and recommendations, highlighted in the aforementioned reviews, which techUK feel the government need to adopt in order to balance consumers' desire for privacy and security with industry's legal requirements to support the security services in their vital work. This will support an ecosystem in which both UK and global technology companies can thrive, create jobs and contribute to the UK's economic growth.

Further information about the Bill and the recent independent reviews into the UK's surveillance regime can be found in the attached FAQ page.

1. Encryption is fundamental for national security and the economic wellbeing of the UK

Encryption is the process of converting information into an unreadable form, so that only someone with the decryption key can read it. It is used to store and transmit sensitive information.

Encryption is fundamental for UK GDP and underpins the fabric behind the digital economy. The internet is now the UK's second biggest economic contributor, contributing £180billion to the overall economy in 2015. Recent surveys suggest that 90% of large businesses and 74% of SMEs suffered a cyber breach in the past year, costing large businesses between £1.46m-£3.14m per breach. Encryption is seen as the best method to ensure that businesses and government are not vulnerable to online attacks and fulfil their legal obligations under data protection statutes to keep personal data free from external intrusion.

According to Mike McConnell (former Director of the US National Security Agency), Michael Chertoff (former Head of the US Department for Homeland Security) and William Lynn (former Deputy Defence Secretary), the undermining of encryption is neither technically nor economically feasible. All three agree that "the greater public good is a secure communications infrastructure protected by ubiquitous (end to end) encryption at the device, server and enterprise level without building in means for government monitoring".[1]

2. Companies should not be placed in an irreconcilable conflict of laws situation

Communication services are increasingly being provided on a global basis. The extra-territorial assertion of national laws such as the Data Retention and Investigatory Powers Act (DRIPA) has resulted in overlapping and conflicting laws that create uncertainty for law enforcement and companies, undermines user privacy and hinders innovation.

Were the draft Bill to re-assert UK law extraterritorially, it would likely trigger reciprocal action from other governments and not achieve the government's policy goal of greater legal clarity. British companies operating abroad might find themselves having to retain and provide data to satisfy overseas governments. It will also remove limits on UK jurisdiction and bring the UK in to conflict with the sovereignty of other countries.

Reforming existing Mutual Legal Assistance Treaties (MLATs) or reaching new international agreements where necessary is the only sustainable, long term solution to addressing complex legal conflicts and gaps between jurisdictions. According to Sir Nigel Sheinwald, the Prime Minister's Special Envoy on international legal frameworks and jurisdiction, improved Government to Government co-operation is crucial to addressing these barriers to lawful disclosure of data across jurisdictions. MLAT reform and/or new agreements provide the best route to a sustainable and coherent legal framework, not the unilateral assertion of limitless jurisdiction. Government should also explore how it can increase transparency around the number and nature of data requests it makes.

3. Case for bulk data must be made

Section 8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA) allows GCHQ to authorise the bulk interception and collection of millions of simultaneous communications on an internet backbone. The question of whether this is necessary and proportionate for the purposes of article 8 of the European Convention is currently subject to review in the European Court of Human Rights (ECHR).

In the US, Congress allowed section 214 of the Patriot Act to lapse and this ended one of the US Government's means of bulk collection of email metadata. The prior debates in the US

[1] 'Why the fear over ubiquitous encryption is overblown', Mike McConnell, Michael Chertoff and William Lynn, Washington Post (July 2015)

legislature questioned the effectiveness of, and need for, bulk data and interception capabilities and found the case to be unproven. In fact, evidence shows that the initial impetus for the majority of counter-terrorism investigations in the US were a result of traditional investigative methods, rather than bulk collection of data.

David Anderson QC made clear that, if bulk data provisions are deemed lawful and parliament wishes them to continue, the case must be made by government and the new Bill should subject these capabilities to strict controls, including judicial authorisation and separate authorisation regimes for bulk data collection and bulk interception. Technical feasibility and due consideration of the costs associated with it must also be considered in any assessment of the operational case.

4. Judicial authorisation of interception warrants will strengthen current safeguards and support greater international cooperation

One of the criticisms of current surveillance practices is that the oversight arrangements in place do not provide adequate protection for users through the involvement of an authority separate from the investigative apparatus authorising and reviewing interception warrants.

The UK can no longer remain isolated from other like-minded countries, such as the US, Australia, Canada and New Zealand, and continue to have political rather than judicial oversight of interception warrants. The surveillance of the content of a person's online communications can be as intrusive as stepping into their house and opening their drawers to read their letters, and as such the level of authorisation required should be equivalent. The introduction of judicial authorisation in the Bill would therefore bring the requirements for interception of digital communications in line with other surveillance practices where privacy intrusion is greatest.

Judicial authorisation is also an important step in facilitating international co-operation between like-minded, democratic countries and will help build a new international framework for acquiring data from other jurisdictions.

5. Greater transparency is essential to re-build public confidence

Since 2010 there has been growing public concern into how surveillance is conducted in the UK, with recent surveys revealing that 72% of British consumers are concerned about their private information online.[2] Small shifts in public sentiment regarding the security and privacy of users' communications can have serious consequences for the UK's digital economy. This is why many companies publish transparency reports for consumers – ensuring that citizens are fully informed of issues related to surveillance and privacy.

These concerns have focused on claims around the prevalence of, and preference for, very intrusive means to access private data. David Anderson QC addressed these concerns in his review and concluded that powers should be set out clearly and comprehensively in primary legislation, with the most intrusive powers limited to specific agencies where there is an operational case and it is also a proportionate and necessary interference with individuals' privacy.

The upcoming Bill can go further than this and commit to a *bias* towards "front doors" as a way of re-building public confidence in the exercise of investigatory powers. By "front doors", techUK mean a commitment to transparent, warrant led procedures and due legal processes. A policy approach based on a bias towards front doors is particularly crucial for providers who have experienced unauthorised access by agencies and/or whose services rely on infrastructure provided by others as this will rebuild public confidence in services that underpin the digital economy.

[2] The research, conducted by YouGov, surveyed more than 2,000 British adults