Response: Investigatory Powers Review: Call for Evidence

About ISPA

The Internet Services Providers' Association (ISPA) is the trade association for companies involved in the provision of Internet Services in the UK. ISPA was founded in 1995, and actively represents and promotes the interests of businesses involved in all aspects of the UK Internet industry.

ISPA membership includes small, medium and large Internet service providers (ISPs), cable companies, web design and hosting companies and a variety of other organisations that provide internet services. ISPA currently has over 200 members, representing more than 95% of the UK Internet access market by volume. ISPA was a founding member of EuroISPA.

We have been involved in the area of communications data for many years, including the passing of the Regulation of Investigatory Powers Act (RIPA), the development of data retention provisions under both the Anti-Terrorism Crime and Security Act (2001) and the Data Retention (EC Directive) Regulations 2009. Most recently we responded to the Joint Committee on the Draft Communications Data Bill and the Data Retention and Investigatory Powers Act. A number of our members are subject to obligations under RIPA and associated legislation.

Introduction

ISPA welcomes the opportunity to respond to the Review of Communications Data and Interception Powers (the Review).

The Review is much needed, not only because the leaked information provided by Edward Snowdon has fundamentally changed public understanding and scrutiny of surveillance issues, but also because of the significant increase in the use of internet communications since the passing of RIPA. What was once a policy issue that received only limited amount of specialist attention, the access to and use of communications data is now a major political issue and one that deserves sufficient time and resources for scrutiny.

ISPA's members accept that law enforcement agencies should have reasonable lawful access to communications data in order to help in the detection and investigation of serious crime and to safeguard national security. However, ISPA members also share concerns raised about the UK data retention regime and recent reform efforts.

Some of the elements of the current regime perform well and should be retained in any future reform programme. For example, the Single Point of Contact System (SPOC) has provided for an

effective means of structuring the relationship between law enforcement authorities (LEAs) and ISPs. The current system also provides for the recovery of the costs that CSPs incur when they comply with requests. It is important that this continues so that CSPs' continued investment in innovation and service development is not adversely impacted by data retention requirements. Cost recovery further acts as an important safeguard as it ensures that law enforcement only requests data where the cost can be justified. It is crucial that these elements continue as part of any future communications data regime. In the remainder of this document, we set out our thoughts on the policy making process in the area of communications data and what we hope the Review will achieve. We further outline a number of principles that should govern any future reform efforts.

Summary of main points

- Since the passing of RIPA in 1999, there has been insufficient consultation with industry and other stakeholders
- Government has failed to facilitate an open debate around communications data and interception and amendments have been made without meaningful scrutiny
- The Review is a first and vital step in ensuring that policy is developed in line with proper process and standards of consultation
- The CJEU's judgment on the Data Retention Directive highlighted the need for data retention regimes to be structured in a way that complies with the principle of proportionality and fairly balances the requirements of law enforcement, privacy of users and the impact on business
- We suggest five principles that should guide policy development in this area:
  1. Data minimisation – Data retention should be limited as far as possible both in terms of data being retained and accessed
  2. Oversight maximisation – Data retention should be governed by a clear legal framework in which executive powers are subject to strong checks and balances
  3. Transparent operation – Data retention risks undermining public trust in communication networks if government does not publish information about the number of requests made to ISPs
  4. Jurisdictional respect - Any data retention regime must allow for a clear, robust and workable system to govern cooperation across jurisdictions
  5. Competitiveness – The impact of a communications data regime must protect the UK's position as an attractive arena for digital businesses

An area that we do not cover in detail in the remainder of the response but that is nevertheless important to us is how Part 1, Chapter 1 of RIPA applies to and affects the day-to-day operation of providers. RIPA was essentially drafted for the world of postal and telephone communications and its provisions make it very difficult to determine whether activities carried out by a provider constitute lawful or unlawful interception. This is particularly relevant in a time where providers are being asked to play a greater role in the protection of their customers, e.g. in relation to the provision of network level parental control solutions or malware protection. This issue should be kept in mind in any reform of RIPA and guidance for ISPs is essential.

Thoughts on the policy making process and what we hope the Review will achieve

The Government's decision to undertake an independent review of the use and governance of communications data and interception in the UK is a marked and welcome change from previous experience. There has been little comprehensive consultation with industry (and we understand other stakeholders) to fully evaluate and review communications data and interceptions powers since the passing of RIPA in 1999. The debate around communications data and interception is also complex and that concerns about security and confidentiality sometimes limit what can be revealed publicly. However, Government should have done more to ensure that policy is developed in an open and transparent manner.

The requirements of law enforcement, privacy of users and the impact on business can only be properly balanced if policy development and political debate are based on a sound evidence base and sufficient time is provided to those who have to make the final decision and those who wish to influence the process. This requires that the Government is open and forthcoming about its aims and stakeholders are given the chance to provide input during both the pre-legislative process and when legislation is discussed in Parliament. Recent debates around communications data demonstrate that this has not always been the case, e.g. in relation to the passing of the Data Retention and Regulatory Powers Act 2014 (DRIPA) and the proposals for a Communications Data Bill.

The Government has insisted that the recently passed DRIPA does not provide for an extension of current powers to intercept and use communications data even though it can be argued that DRIPA allows the new application of RIPA powers to communications services and entities both within and outside the UK that were not clearly covered by the previous legislation. By framing the debate in such a way and by relying on an accelerated parliamentary process, the Government has

effectively created a situation where Parliament has passed a new Act without being able to have a thorough and informed debate.

While the Joint Committee on the Draft Communications Data Bill extensively consulted with stakeholders, it is still the case there was only limited meaningful consultation as Government did not allow for any structured input during the actual drafting process. This was recognised by the Committee which concluded that more consultation with industry, technical experts and others was needed and that meaningful consultation can take place only when there is "clarity as to the real aims of the Home Office."[1] Even though the Joint Committee's very clear conclusion was accepted by the Home Office, there have been no further attempts to properly consult with industry, even with the introduction of DRIPA which, in the eyes of some observers, significantly extends capabilities in certain areas. Government may argue that it does meet with stakeholders but we contend that it is not conducted in a properly open and comprehensive way.

We see the Review as a first and vital step in ensuring that policy is developed in line with proper processes and standards of consultation. Given the complexity of RIPA and the Government's approach to consultation, it is no surprise that the policy process has at times failed to fully engage with the intricacies and implications of some of the reform proposals that have been made in recent years. Going forward, Government needs to foster a full and informed debate by:

- Developing policy within an open and transparent framework
- Allowing time to debate complex issues fully with all stakeholders, including industry and civil society and user and human rights groups
- Being clear about the scope and aims of reform proposals

Five principles for achieving a better communications data regime

In its recent judgement, the Court of Justice of the European (CJEU) declared the European Data Retention Directive invalid. Whilst the judgement does not directly apply to the UK data retention regime we believe that it provides a useful starting point for considering a number of principles which should govern any future reform efforts.

The CJEU found that by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data. The Court also found that the fact that data are retained and subsequently used without the subscriber

[1] Joint Committee on the Draft Communications Data Bill (2012), Draft Communications Data Bill, p. 75

or registered user being informed, it is likely to generate a feeling that their private lives are the subject of constant surveillance.

While the Court accepted that the Directive satisfies an objective of general interest (namely the fight against serious crime and, ultimately, public security) it ultimately failed to comply with the principle of proportionality by failing to ensure that the interference with fundamental rights (e.g. right to private life and to the protection of personal data). The Court touched on a number of issues and the following are of particular importance:

- Coverage, in a generalised manner, of all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.
- Failure to lay down any objective criterion which would ensure that the competent national authorities have access to the data and instead simply refers in a general manner to 'serious crime' and does not require any prior review by a court or by an independent administrative body.
- Lack of objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.

It is not for ISPA to undertake an in-depth legal assessment of the UK data retention regime on the basis of the CJEU judgement. However, the key issue going forward will be to ensure that the UK data retention regime takes account of the judgment and is proportionate and fairly balances the requirements of law enforcement, privacy of users and the impact on business. The following principles should guide policy development:

1. Data minimisation – Data retention should be limited as far as possible both in terms of data being retained and accessed
2. Oversight maximisation – Data retention should be governed by a clear legal framework in which executive powers are subject to strong checks and balances
3. Transparent operation – Data retention risks undermining public trust in communication networks if government does not publish information about the number of requests made to CSPs
4. Jurisdictional respect – Any data retention regime must allow for a clear, robust and workable system to govern cooperation across jurisdictions.
5. Competitiveness – The impact of a communications data regime must protect the UK's position as an attractive arena for digital businesses

Data minimisation

While it may not be possible for law enforcement purposes to disclose exact details of who and what is being subjected to data retention, the current data retention regime in the UK allows for the blanket collection of communications data for virtually any communications service and risks undermining public trust in modern communications media. The use of broadly defined reasons to justify the access to data, e.g. "preventing or detecting serious crime" also does not provide sufficient safeguards to ensure that the private data is being used in entirely appropriate ways. With this in mind, we believe that the data retention regime should codify sensible limitations on Government's ability to compel service providers to retain and disclose data. Limits should apply in relation to:

- the types of data subject to retention;
- the individuals subject to retention; and the
- purposes for which the data can be disclosed and accessed.

We would particularly welcome if the Review explored more targeted means of capturing and accessing communications data. For instance, the viability of relying on data preservation rather than retention as a means to limit the number of individuals that are directly affected by data retention. Additionally, clear legal barriers should be inserted in the acquisition process for communications data to ensure that data is not provided without a full assessment and balancing of competing rights. This is particularly relevant for cases where RIPA can be used to acquire information about whistle-blowers, sources of journalists or conversations between doctors/journalists and their clients. It reaffirms the need to clarify the definitions of serious crime and national security that RIPA was originally intended for and the need to impose clear limitations on where RIPA should not be used.

Oversight maximisation

Communication is more data driven than ever yet the UK still relies on a data retention regime that was essentially drafted to regulate the retention and use of communications data for telephony and email communication. The privacy impact of communications data generated by modern communication services, such as social networking, can be more revealing than the more traditional services. It is therefore crucial to consider the ability of law enforcement and other competent authorities to combine data sets from different communication services which again may have a more severe privacy impact. As such it is vital that oversight mechanisms are able to keep up with technological developments. With this in mind, we believe that any data retention

regime should be governed by a clear legal framework in which executive powers are subject to strong checks and balances. This implies that:

- Parliament needs to be enabled to have an informed debate and make an informed choice before and after relevant regulations are passed;
- Mechanisms for the day to day oversight are well resourced fully independent and effective; and
- Mechanisms are provided to clarify the law where powers are not clear or disputed.

We would particularly welcome if the Review investigated how the existing oversight mechanisms can be strengthened and improved. Aside from providing more resources and recruiting Commissioners from a more diverse set of candidates, the remit of the oversight bodies could be expanded. Instead of merely spot checking whether the proper processes for the retention and acquisition of communications are adhered to, Commissioners could seek to undertake a more in-depth assessment of whether powers are used correctly and whether the rights of users are properly balanced with the interests of law enforcement. This would be particularly relevant if Government decided to extend its capabilities in line with the proposals for the Communications Data Bill. To assist with this, Commissioners should utilise expertise from industry, law enforcement, user groups and human rights representatives to challenge and inform working practices and processes, e.g. through a formal advisory board. There may also be merit, either within or outside the existing oversight bodies, in allowing users and providers to clarify the law where powers are not clear or disputed, e.g. if existing powers are applied to a new service that may allow access to data with greater privacy impact.

Transparent operation

Transparency is crucial for maintaining public trust in modern communication networks and underpins the whole debate around data retention. Oversight mechanisms are strengthened if their findings are publicly available and can be subjected to an independent assessment. Public trust can be maintained if meaningful information is provided about the scale of data retention. This implies that:

- Government should allow oversight mechanism to publish detailed information about the number and nature of government demands for user information and about the day-to-day operation of the communications data regime
- Government should allow private companies to publish the number and nature of government demands for user information if they wish to do so.

Jurisdictional respect

The global nature of Internet services means that international cooperation is vital. Any data retention regime must allow for a clear, robust and workable system to govern legal requests across jurisdictions and protect existing good cross-border relations. In doing so, the regime must:

- Respect existing jurisdictional arrangements and international law and where necessary review improve existing arrangements, e.g. MLATs in the first instance
- Require Governments to work together to address issues with access to data with the goal of providing clear legal frameworks which provide certainty for providers
- Provide mechanisms for ensuring requests from LEAs are proportionate and necessary, and not overly broad or framed in a way that would circumvent the laws of the UK or other countries.

Competitiveness

The impact of a communications data regime must protect the UK's position as an attractive arena for investment, development and growth of digital businesses – one of the most important sectors to the UK economy. The Internet sector is constantly innovating to offer customers new ways of communicating and consuming or producing content, often led by start-ups. There is a real danger that these services and providers could be subject to communications data retention requirements, fundamentally changing how these (often small) businesses operate. There is also a danger that due to jurisdictional issues, UK providers are asked to retain data of overseas third party services that is transmitted over their network which would further disadvantage them in the market place. To limit damage to competitiveness and innovation the regime must:

- Provide clarity over what data is in scope and empower Parliament and independent oversight bodies to help define this data;
- Include comprehensive and transparent impact and cost assessments; and
- Minimise the possible damage to CSPs and the UK as a place to do business.

It is worth adding that due to the extra-territorial application of the UK regime, other countries, including those with more authoritarian regimes, may feel entitled to not only enact similar data retention powers but also apply to them to operators purely operating in the UK. The review should factor in that UK policy in this area is developed and replicated elsewhere.

Conclusion

The Internet is fundamental to how we live our lives; not only is it a primary means of communication, it underpins the economy and is a real engine for growth and change. It is vital that policy decisions made in the area of communications data and interception do not undermine

trust and security in modern communications networks. The UK must adopt a regulatory framework that works for law enforcement, users and industry and we have set out five principles to guide the reform process.

The Review is a first step in ensuring that the wider policy is developed in line with proper process and standards of consultation. However, we are concerned that the debate around communications data could once again become politicised and urge all political parties to take account of the independent Review's findings instead of falling back on already established policy positions. Achieving a regime that manages to proportionately balance competing interests is a challenge but getting it right will help the digital economy to continue to thrive and innovate whilst maintaining the ability to investigate serious instances of crime.