Internet Telephony Services Providers' Association

Response to the Joint Committee on the Draft Communications Data Bill

About ITSPA

The Internet Telephony Services Providers' Association (ITSPA) is the UK VoIP industry's trade body, representing over 60 UK businesses involved with the supply of VoIP and Unified Communication services to industry and residential customers within the UK. ITSPA pays close attention to the development of VoIP and IP regulatory frameworks on a worldwide basis in order to ensure that the UK internet telephony industry is as competitive as it can be within international markets.

Please note that certain aspects of the ITSPA response may not necessarily be supported by all ITSPA members. Individual members may respond separately to this call for written evidence where a position differs.

A full list of ITSPA members can be found at http://www.itspa.org.uk/

As the joint committee will understand, it is difficult for a trade association with a broad membership to respond to each individual question with a uniform answer. Members have different experiences surrounding data requests from law enforcement and local authorities and different positions (based on the services they supply) on the proposed legislation put forward by the Coalition Government. We have responded in general terms, following several discussions with our members and highlighted specific points of concern and interest which we hope the Joint Committee can investigate further. ITSPA members would welcome the opportunity to discuss specific points at greater length with the Joint Committee, should it be deemed necessary.

General Comments

ITSPA welcomes the opportunity to provide written evidence to the Joint Committee on the Draft Communications Data Bill. It is an important piece of legislation that needs to be scrutinised effectively to ensure a workable process can be implemented. Law enforcement organisations must have access to the communications data they need to tackle serious crime, however the communications industry must not be overburdened with a regime that causes operational difficulties or infringes on their customers'

privacy. Whilst ITSPA accepts the sensitive nature of some of the issues surrounding this legislation, the confidential nature of some areas have made it difficult for our members to respond as comprehensively as we would like. We would urge the Joint Committee to gain greater detail from the Home Office in order to provide industry with greater clarity of the long term implications of the draft Bill.

The main concerns for ITSPA members in terms of scope are the precise type of data sets that will be required in the future and the exact requirements surrounding both third party data and compliance of overseas providers. These are key areas that we believe the Joint Committee should focus on to ensure the proposals can work in practice.

Law Enforcement Requirements

As previously mentioned, ITSPA recognises the importance of communication data for law enforcement agencies as they seek to prosecute crime. We accept that the way people (and criminals) communicate is shifting, due to changes in technology. It is important that law enforcement keeps up with these trends. ITSPA members cooperate fully with the data requests under the existing legal framework.

From an initial perspective, particularly for 'pure' VoIP providers (those providing only IP telephony and not other services like instant messaging), there would appear to be only minimal changes to the current obligations. However we do have concerns surrounding any future requirements that this Bill may bring on the VoIP industry, which is not clear in either the content of the draft Bill or in discussions with the Home Office. There appears to be a lack of clarity as to whether other data sets (not retained for normal business purposes) will have to be retained by telecommunication providers in the future and it is therefore hard for ITSPA to make an assessment of the long term implications for the industry. We accept our responsibilities to support law enforcement agencies but the relationship must be built on trust and effective communication as to how this legislation may affect the industry going forward.

We would also question the suggestion that this draft legislation is merely maintaining current capabilities for law enforcement agencies. Whilst it is true that the draft Bill is focussed on bringing new technologies into the scope of the current regime, there are a number of other areas that strongly suggest an extension of scope. These would include the new filtering arrangements, retention of third party data and the changing of definitions surrounding communications data and telecommunications providers. This does not necessarily impact the majority of our members (at least in the short/medium

term) but it will certainly have an impact to the wider communications industry and could potentially impact VoIP providers in the future. This is why ITSPA requests further clarity on the proposals involved and we would ask the Joint Committee to investigate further.

Filtering Arrangements and Technical Issues

There are also significant concerns as to how a filtering system would work without significantly disrupting communication providers' (CPs) operations, inadvertently capturing communications content, and/or creating dangerous opportunities for the leakage of sensitive data or data fraud.

ITSPA would welcome further investigation into how data will be collected under a notice and how the filter will interact with the CP. There have been suggestions that the Home Office may require a direct feed to the providers' data base. This could cause a number of problems in terms of both consumer data security and for the operations of a CP. There are also question marks surrounding how the interaction with the filter will be affected by any network upgrades or configuration changes that the CP may need to undertake. This could cause both operational problems and have financial implications for the CP; it is unclear as to whether this element of cost recovery would form part of the Home Office's new obligations. Equally there are competition concerns around this point. CPs who have not received a notice and do not interact with the filter, will not be hampered by the potential hazards surrounding network upgrades. Further information on how the filter would work is vitally important. ITSPA members would be concerned if a similar system to the Netherlands was adopted, whereby CIOT (the authority responsible) can require that registered communications providers install a direct feed into their servers so that CIOT can download data every 24 hours. We believe that the Dutch arrangement is not proportional to the need and can result in serious implementation issues for CPs.

In terms of some of the technical queries outlined, ITSPA does believe that there are vendors who are able to offer the solutions to capture the necessary communications data. However, the safety and security concerns cannot be underestimated. It would be an extremely challenging process for the industry to undertake. CPs would be obligated to ensure third party data was captured and that the filter could cope with enormous volumes of data. Such data, when aggregated, becomes important and extremely sensitive information, which increases the business impact level and security threat. Some data

may include government data up to the Restricted level (as is allowed over the ISDN). The costs of storing such data can be prohibitive and the risks must be evaluated properly.

Costs

ITSPA does not believe that the Government estimate of £1.8bn over 10 years is realistic. We feel there are too many factors that may contribute to this cost rising significantly. It could cost large CPs hundreds of millions of pounds to integrate and store data correctly, to include third party data and other information that they would not usually store for business purposes. Over time, as data requests are made to smaller providers, the extra costs will also filter down, creating a significant financial burden.

There is also an assumption by the Home Office that access to data from overseas providers will be relatively straight forward. ITSPA members are less convinced this will be the case and we believe the costs could be higher than estimated. Future developments and capabilities within the communications space will also mean that law enforcement agencies may have to shift their focus to other methods of communication and this will inevitably mean a stark increase in overall costs.

We welcome the Home Office's commitment to cost recovery and would stress this as a requirement for any final legislation. This commitment is fundamental to ensure an effective system is maintained. Whilst ITSPA has not had insight into how the Home Office has costed their proposals, we fear the projected figures are too optimistic, given the technical challenges that the wider communications industry may experience.

In terms of cost benefits, ITSPA does accept that there could be considerable savings and suggest that this could even exceed the £5-6bn suggested. The more effective the communications data that law enforcement agencies receive, the more efficient they will become in solving crimes, catching criminals and coping with major incidents (such as public disorder). This will create financial efficiencies within the respective organisations and reduce the financial loss that both individuals and organisations experience when they are victims of crime and fraudulent activity. However, as previously indicated, ITSPA does expect the costs to implement these changes to be more expensive than predicted which needs to be taken into consideration when deciding the true value of the draft Bill for both law enforcement organisations and society as a whole. Given the economic constraints on Government at present, there is a need to ensure the financial costs are truly going to bring tangible benefits.

Internet Telephony Services Providers' Association

Safeguards and Oversight

The filter will have access to an enormous amount of data and will need some strong controls to prevent misuse and protect against criminal hacking. There is also the concern that it will be unavoidable in some instances to prevent collating content. Certain information required by enforcement agencies will contain content embedded in the data that cannot be removed without destroying the data. For example, in web access logs the destination urls can contain information that discloses the nature of the content.

ITSPA feel that in terms of the existing communications data that is stored or for data that is anonymous, the safeguards currently in place would be sufficient. However a warrant system should be considered for data that included content when it was not possible to supply anonymous access data without rendering the data meaningless.

In terms of everyday oversight, ITSPA members are generally happy with responsibility being devolved to the Interception of Communications Commissioner's Office (IoCCO) and the Information Commissioner's Office, provided they are sufficiently resourced and have the technological understanding of the services being used. There have been questions raised by some members surrounding the amount of parliamentary oversight to the draft Bill and whether too much power will lie with the Home Secretary in this area once legislation is passed.

ITSPA members are satisfied that the sanctions currently in place under the present regime will be sufficient under any revised legislative framework.