Investigatory Powers Bill: technology issues

submission by Exa Networks Limited

by

Thomas Mangin

Technical Director

26 November 2015

# Executive summary

1. We have concerns and reservations regarding the technical impact of the extension of interception requirements placed on networks.
2. We have reservations regarding the estimated cost of collection and storage of Internet connection records as currently defined in the financial implication of the bill.
3. We note that the extension of the reach of UK law may create an environment where UK business may not be able to source some services from foreign organisations or at competitive price in the UK.
4. Any interception method should be proportionate, targeted and subject to full legal supervision to keep the technical and financial impact of such measures under control.
5. We believe that the bill would weaken and worsen the competitiveness of the UK technology industry as it affects privacy protection, such as encryption and the ability to use equipment free of interference.
6. The bill includes wording which may make future discussion surrounding data interception very hard, if not impossible, by preventing service providers from discussing their interception capability.

# About Exa Networks

1. Exa Networks is an Internet Service Provider incorporated in 2003.
2. We provide mainly connectivity solutions to the education market.
3. A large part of our activity is real time filtering of schools’ internet traffic.
4. Exa Networks developed a system capable of recording the web activity of its education customers similar to what the bill proposes but more limited in scope.
	1. This system, a unique selling point, does account for a large account of our R&D and internal cost of service delivery.
	2. This system does significantly increase the cost of our connectivity services.
	3. and would cost considerably more should more feature and long term storage requirement be added.
5. While Exa Networks is not currently enrolled in any governmental data collection scheme, it may be requested to be.

# Comment about the bill and consultation

1. Previous bills have seen interpretations which granted wide ranging power to the government. Some of the definitions of the bill do not seem to accommodate the complexity of Internet Protocol networks.
2. The time frame for this consultation was very short and therefore Exa Networks is not able to provide any detailed answers on some of this very complex bill.
3. The bill defines a new set of definitions, which makes it much harder for organisation to understand the scope and reach of the new power being sought by the government.
4. The bill contains wording which would prevent service providers from discussing their interception capacity.
5. This would reduce the opportunity for service providers to discuss
	1. best practices and
	2. provide accountability on their operations and
	3. improve the cost effectiveness or interception.
6. Service providers already collaborate with law enforcement under the current regime which allows Service Providers to verify the validity of interception requests.
7. Any interception method should be proportionate, targeted and subject to full legal supervision to keep the technical and financial impact of such measure under control. This bill does prone the collection of data from innocent citizens.

# The technical feasibility and costs of meeting the obligations imposed by the Bill

1. Exa Networks Limited does collect information as part of its normal operation which has over time been requested by law enforcement personal.
2. Exa Networks Limited is not currently under any obligation to perform any interception therefore we:
	1. have no knowledge of how this interception is currently performed by Service Providers
	2. can not rely on current costing to extrapolate the impact of the bill.
3. The bill requires organisations to collect new data which is not already intercepted or stored for “business as usual”.
4. It requires the installation and maintenance of equipment which are not currently present in networks.
5. The bill does draw a difference between communication data (ICR, Internet Connection Record) and content data
6. It requires interception of information which requires that service providers analyse the content of data to know what should or should not intercepted.
7. Technologies permitting the categorisation of the information, in order to extract meta-data only, are extremely expensive as they need to work on all the information passing through the network.
8. Even while using these technologies, some forms of communication are protected from inspection using obfuscation, and therefore will not be able to be made legible.
9. Some form of obfuscation may use patented technology, making the decryption illegal under reverse engineering and/or patent law and possibly placing the service provider at risk of litigation.
10. It is extremely hard to decode information which has been intentionally protected against interception, and extract meaningful intelligence from it.
11. The financial implication does not consider the cost of following the evolution of technology, some of which may be in reaction to the bill itself, to keep interception capacity relevant and costs under control.
12. It is likely that privacy friendly organisations will continue their work to make the collection of the data harder.
13. For example, google protects its connections, it is therefore impossible to reliably say if a user made a web search or used any other of the service google provides such as mail, maps, social chat, etc.
14. Most large consumer web services are actively working to promote secure web browsing and make their service hard to intercept.
15. The current browser trend is toward generalised cryptography deployment with new features to make all interception harder.
16. Most communication services (like mobile chatting) work in ways where it is not possible to know when and where messages were exchanged, and with whom.
17. Unlike the telephony network, the distinction between Signalling and Content is not clear and easy to establish.
18. As collection is to affect every communication of every UK citizen, the level of data which would need to be collected is unprecedented.
19. This data will need to be stored for 12 months, adding an additional storage issue.
20. No publically published study was carried out, and peer reviewed, to try to evaluate the storage need the legislation is proposing.
21. The data gathered must be searchable which requires the creation of more data, and use of more equipment, to be able to perform such a search.
22. Providing effective search features on the scale presented presents many technical challenges.
23. The stored communication data must be kept secure.
24. No commercial product currently provides a turn key solution for such secure storage with search features.
25. The current text seems to give the government the option to create a meta-search engine, ie: software which will be able to query data collected by multiple service providers.

# The **impact** on communications service providers and related businesses

1. Implementation of the bill would require a significant amount of engineering time to install new interception equipment.
2. Such work would have a direct impact on
	1. the ability of the business to complete its current roadmaps (product, engineering),
	2. capacity to cope with growth as resources would need to be diverted to install the interception capacity.
3. The bill will result in a reduction of the IT service provided by the UK aboard which are serviced by UK internet service providers.
4. The bill does not limit its scope to UK organisations but any organisation providing services to UK residents.
5. Any UK organisation selling aboard will have to compete with organisations which
	1. do not have to carry the cost of the bill
	2. can provide more privacy guarantees against traffic inspection
6. This will affect the willingness of some business to operate in the British Islands
7. It will increase the complexity of compliance for
	1. activity logging
	2. securing computers against malicious data

as these activities will not be able to be performed centrally in the network.

1. The implementation of the interception as defined in the bill will reduce the competiveness of UK businesses.

# The likely consequences for **citizen/consumer** use of ICT services

1. The bill will increase the cost of broadband services in the UK as it is very unlikely that the government will be able to fully cover the cost of such interception
2. Consumers may lose trust in UK products which may have been interfered with to allow some form of communication interception.
3. Citizens are likely to increase their use of encryption, making communication data much less useful and relevant
4. It may reduce the level of investment in UK technology companies
5. UK ICT companies may prefer to purchase services from foreign companies not required to implement the bill.
6. The UK industry needs to be able to be able to use strong privacy protection such as encryption and be able to use equipment free of interference to keep its business and the country secure, the bill would prevent UK business from doing so.
7. UK law should only apply to UK registered business. Any extension of the reach of UK law may create an environment where UK business may not be able to source vital required services at a competitive price.
8. The bill includes some wording which will make future discussion surrounding data interception very hard, if not impossible, by preventing service providers from discussing their interception capability.