When it comes to Internet security and privacy, the public remains confused

January 14 2016, by David Glance, University Of Western Australia

Encryption. Credit: Christiaan Colen/flickr, CC BY-SA

The UK government is proposing to follow Australia with the introduction of their version of data retention legislation called the Investigatory Powers bill. This will require Internet Service Providers (ISPs) to maintain records of web addresses customers visit for a period of 12 months (in Australia it is 24 months).

The legislation has been opposed by much of the tech industry including Facebook, Google, Microsoft, Twitter and Yahoo acting as the "Reform Government Surveillance" alliance. Companies are largely concerned that anything that diminishes their customers' trust in the companies' ability to protect a user's privacy will diminish their trust in the companies concerned.

A survey released this week from Broadband Genie, a UK ISP, suggests that the public may have changed its mind about the importance of government surveillance. 63% of the respondents said that they supported the changes to surveillance laws to protect the country. 27% of those who supported the proposed legislation had done changed their minds as a result of recent terrorist attacks such as the one in Paris.

Unfortunately, those surveyed were less convinced that ISPs could be trusted with the job of storing the retained data securely. Only 33% believed that their ISP could store users' data securely.

It is worth being cautious about over-interpreting one survey, especially when it is not known if those answering really understood the full ramifications of the proposed legislation. They may not be aware of the arguments for, and against, data retention, and certainly have little means of assessing the relative risks of any of the potential pitfalls of storing this type of data.

The public's perceptions of the importance of privacy changes however when it comes to smart home devices known generally as the "Internet of Things". In a large, world-wide survey of 28,000 consumers, Accenture has reported that 47% of respondents reported concerns over security and privacy as a major barrier to purchasing Internet of Things devices and services. Of those people who owned or were planning to buy devices, security concerns resulted in 79% deciding to postpone purchase of devices (24%), be more cautious in their use of the devices

(37%) or stop using them altogether (18%).

Interestingly, governments are sending very mixed messages when it comes to privacy and security. When it comes to the Internet of Things, the US Federal Trade Commission (FTC) has been very vocal about the importance of protecting the privacy and security of Internet of Things users. This would necessarily involve end-to-end encryption, a feature that the UK's Investigatory Powers Bill seeks to curtail, or at least make its override a feature available to the Government.

The general public could be forgiven for being confused given the contradictory messages coming out of different parts of government organisations. The other complicated factor is that it may not be possible to guarantee privacy and security for consumers whilst at the same time allowing government agencies unrestricted backdoor access to communication.

The truth is however is that neither side can really say with any certainty what is the best path to take. There is merit to both sides of the argument in terms of what possibly might happen if this legislation gets put in place. On the one hand, it is possible that it will make it easier to deal with terrorist threats or events. On the other, it may just force the terrorists to use custom encryption tools that are not subject to any restrictions and worse, result in those same terrorists being able to undermine the security of the very public the governments seek to protect.

In amongst all of this are the attitudes of the public which in the absence of real understanding and evidence, will be swayed by events. Terrorist attacks like the one in Paris or in Jakarta will sway more of the public to agree that governments need to be able to intercept and disrupt terrorists networks using everyday secure communications. Events like the shutting down of power plants in Ukraine by hackers will push the public

the other way into wanting more security of Internet-connected devices - especially those controlling key national infrastructure.

There is little doubt that legislation like that proposed in the UK will become law. Neither side will get what it really wants, and the public is likely to stay confused.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation