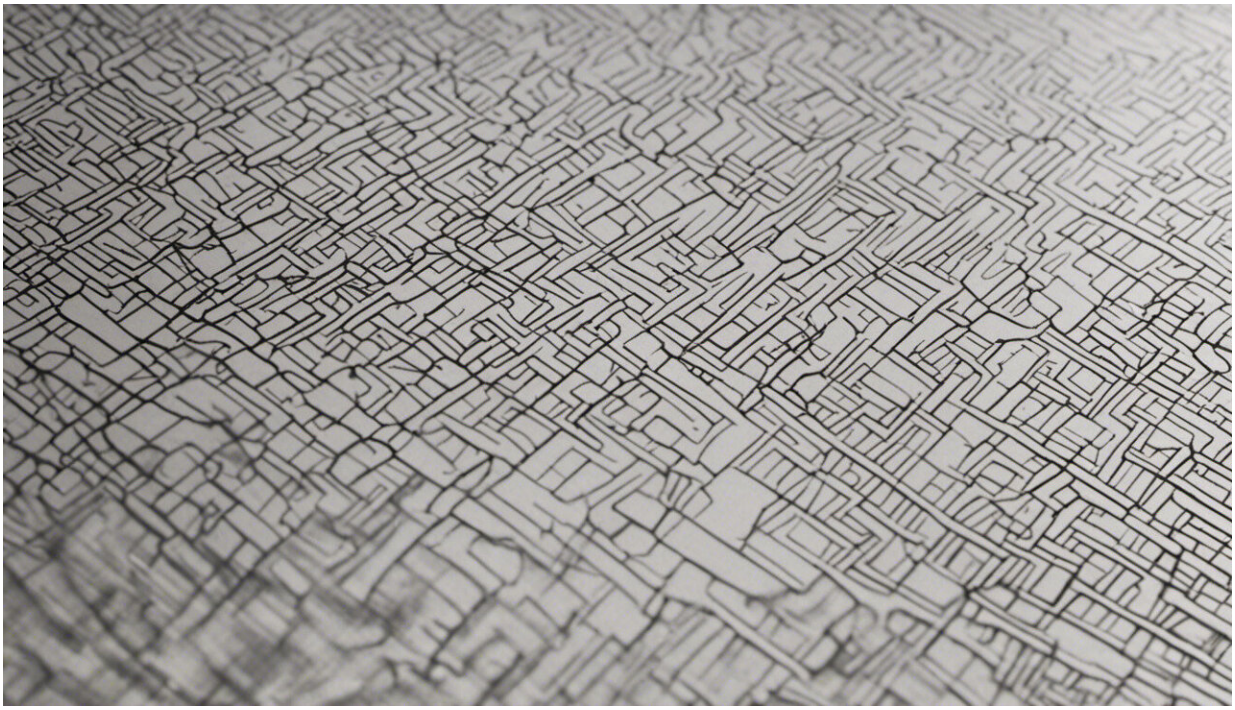
How much of your privacy will you forfeit to ensure your safety?

December 1 2014, by Carsten Maple



Credit: AI-generated image (disclaimer)

The Counter-Terrorism and Security Bill introduced in the UK parliament this week is designed to place legal requirements on certain businesses to retain information about user communications. It has its roots in the previously scuppered Communications Data Bill – the so-called "snooper's charter". The timing of the new bill also coincides with

the publication of a report by the Intelligence and Security Committee into the killing of Fusilier Lee Rigby, which suggested that greater government access to online communications might have prevented the death of Lee Rigby.

There are three sides to this issue. Government and law enforcement say they need as much access to intelligence as possible to prevent serious crimes. The view of much of the industry is that the cost of retaining, collecting and analysing data is massive – hundreds of millions of pounds they argue. And finally you and I have our say, and we want the right to some privacy.

Snooping is legal

The UK government already has a mechanism to access data, but is bound by the Regulation of Investigatory Powers Act, which allows public bodies, such as MI5, to demand that a service provider gives access to someone's communications data, or indeed to intercept a communication. The act is designed to protect the privacy of individuals and requires authorisation – usually by a senior member of the body making the request – before the body can demand information from the service provider.

Authorisation can be requested for a range of reasons, including assessing or collecting tax. MI5 would normally use the act to request assistance of the service provider because it is in the interests of national security, because it will prevent or detect a crime, or because it is in the interests of the economic well-being of the UK.

Hence the government does have a method, albeit there are jurisdictional issues, to demand information from service providers. If the service provider is based outside of the UK issues arise. Legislation passed in the UK does not have direct effect outside the jurisdiction. UK

authorities rely largely on the goodwill of companies to co-operate, or need to use what are called Mutual Legal Assistance Treaties, which enables co-operation between states for obtaining assistance in investigating or prosecuting criminal offences.

Beyond the routes of accessing information, a greater problem lies in authorities requests for such data. If the government doesn't request specific information, the service provider does not have clear understanding of what information it must gather.

Information ≠ Intelligence

There is a phenomenal amount of data being produced globally every day. Given this amount of data, it can be a real challenge to turn this into intelligence.

Data are the raw zeros and ones that are transmitted, to turn that into information means we have to look at the meaning of the transmission. Service providers already do this by automated procedures, and it was such a procedure that led to the closing of a number of Facebook accounts that belonged to Michael Adebowale, Rigby's killer.

Intelligence is putting information into context so that judgements can be made. Even if a service provider provides information to intelligence agencies, there is no guarantee that the information will be used in a timely manner, or used to draw the correct judgement. For this reason we need to be careful at how much responsibility we place at the feet of Facebook for the events leading to Rigby's murder.

It is clear that any new legislation will place greater responsibility upon businesses to store and disclose information. Clearly service providers have been reluctant to perform detailed analysis on the data for the government.

However, businesses already possess technology to gather business intelligence, and that is a core part of their offering to advertisers. Analysing customer behaviours can alert a supermarket that one of their customers is pregnant before the person themselves even knows. The argument that storing the information for longer is more costly, is of course true, but the cost of storing information is continually decreasing. Given that service providers have intelligence techniques and many are generating vast profits, is it acceptable for them to argue so strongly against the bill? Do they not have a corporate social responsibility to do more?

Public should have the final say

The final view on the whole matter is that of the general public. We have a right to some level of privacy. Public confidence in the intelligence agencies and their access to personal data has dropped in the wake of the revelations by Edward Snowden.

However, while we are demanding privacy, we are currently making unprecedented amounts of data publicly available ourselves. This privacy paradox is a result of the fact that we fail to recognise the true value of the information we are publishing ourselves. While we are debating the regulation of surveillance and intelligence methods, there is a significant amount of effort being put into what is termed, Open Source Intelligence . So we need to think clearly about whether we are trying to genuinely protect information or just trying to keep intelligence agencies accountable.

There is a fine line between our right to privacy and ensuring public safety. What needs to be recognised is that there needs to be appropriate oversight of any information collection that ensures the proportionality of ensuring public safety over our rights to privacy.

What is really called for is a consultation on the bill. The trade-off between national security and public safety versus the right to privacy is an important debate and a better understanding is required. Parliament is supposed to act in the interests of the public, and currently there has been no open discussion of this issue.

I don't mean that there should be a referendum, but there needs to be clear information presented to the public, rather than relying on the public reacting strongly in the wake of a single incident.

This communications data issue has been with us for a while and there has seemed to be a concerted effort to open debate about the problem. It is a serious issue and the status quo is not acceptable, but you cannot compromise the rights of the public without making clear the balances of privacy versus security.

Source: The Conversation