« Return to article

Print this

The Straits Times
www.straitstimes.com
Published on Jun 19, 2013

BY INVITATION

Getting used to a surveillance society

Outrage at the United States National Security Agency's collection of data misses the point: The focus should be on how the data is being used.

By Simon Chesterman For The Straits Times

HOW should we balance liberty and security?

The answer is simple: We shouldn't.

The metaphor of a "balance" between liberty and security offers an attractive way to view the current debate over massive amounts of data being gathered by intelligence agencies and the impact on personal privacy, following whistle-blower Edward Snowden's revelations.

"Balance" is used by both civil libertarians and security hawks to suggest a sliding scale in which we can choose more liberty or more security.

But the metaphor is disingenuous, misleading and a recipe for bad policies.

In the breathless coverage of revelations from the US National Security Agency (NSA) leaked by Mr Snowden earlier this month, pundits and lawmakers have professed themselves to be shocked, to find that American intelligence agencies have been spying on people in the United States.

The outrage is echoed around the world, with citizens in other countries questioning if their own governments are also tracking their calls and e-mails.

The surprise is disingenuous because we have known since Sept 11, 2001 that the main threat of politically motivated violence today comes not from an outside aggressor state, but from a terrorist operating within our borders.

Dig a little deeper and the outrage is often revealed to be the fact that the spies are watching "us" rather than "them".

Yet the days of surveillance limited to individual targeting of known terrorist agents are long gone. When security agencies no longer know who "they" are, it is far more rational to gather data on everyone in the hope of looking for behaviour that might suggest, for example, someone planning to pilot a plane into a skyscraper or detonate an explosive device at a major sporting event.

In the past, liberty was protected by reducing the acquisition of data, limiting its retention, and constraining its dissemination.

Given the proliferation of data and the speed and ease of retaining, retrieving and sending information, these constraints are no longer workable.

That is why defenders of the NSA programme shouldn't argue about "balance" either. They know the scales have already been flipped over.

In part this is because our technology has far outpaced our laws. Why should government be prevented access to the data that our smartphones have been gathering on us for years?

There are still some restrictions, to be sure. Though the NSA collects the metadata of communications

between citizens within the US, a warrant is still required to view or listen to the contents. But non-citizens and those outside the US are fair game.

Extraordinary powers

IN OTHER countries such as Singapore, there are still fewer limits on government surveillance, as no court order is required to intercept telecommunications, including the content.

Both regimes allow government authorities to compel technology and communications companies to hand over user data.

Google's Transparency Report, for example, shows that last year, the Singapore Government requested user data on 185 occasions, with Google releasing some data around three-quarters of the time. The US made 16,407 such requests with 90 per cent leading to some data being released.

These are extraordinary powers to entrust to any government, bringing with them the possibility of abuse.

Indeed, Mr Snowden has claimed that he leaked information about the NSA programme because of concerns about abuse.

He highlighted one kind of abuse, which was that a rogue analyst - himself, for example - could spy on anyone he chose, "from you or your accountant to a federal judge to even the President, if I had a personal e-mail".

Such claims appear to be exaggerated.

Established intelligence agencies have protocols to deal with misbehaviour and checks that make it difficult to deploy national security resources for personal reasons - to spy on one's ex-wife, say, or an unpleasant neighbour.

The problem with profiling

BUT there is another kind of potential abuse that is more likely to happen. This is when liberties of a certain section of the population may be compromised more than others.

Take the most prominent example of such potential abuse: profiling, which is implicit in the very notion of systematic surveillance.

Analysing massive amounts of data requires the choice of factors that will flag certain behavioural patterns for greater scrutiny, and particular individuals for further investigation.

Historically, profiling has meant the use of ethnicity as a key factor in determining whether to deploy investigative resources against a particular group or individual. Profiling raises legitimate concerns about explicit or implicit racism and other forms of bigotry, such as when African-American men are more frequently stopped by US traffic police for "random" searches.

Though it has barely been mentioned in the current furore over surveillance, profiling should be front and centre of the debate - and shows how a search for "balance" can be misleading.

Profiling is clearly a part of the investigative method currently used by police and intelligence officers.

The debate often sets the civil liberties of the profiled group against the security interests of the population as a whole. This is sometimes presented in hyperbolic terms, such as that the choice is between profiling and "lost lives".

A better analysis is that the use of ethnicity or religion as a basis for profiling imposes a cost on innocent members of the targeted group. It might be preferable to distribute that cost more equitably, perhaps by excluding the factor perceived as relevant but offensive, and increasing the scrutiny of the population as a whole.

This is where the "balance" metaphor - that gains for liberty necessarily entail a loss of security and vice versa - leads to bad policies. For it obscures the fact that liberty may in fact contribute to security.

In the case of profiling, for example, pre-selecting all young men of a particular faith or ethnicity might well

offend public "sensitivities". But it may also exacerbate the problem that it is intended to solve.

During the Bush administration, reference to a "global war on terror" - a term now rightly abandoned - falsely implied that groups with diverse aims and widely varied capacities were in fact part of a worldwide conspiracy pitted against the US.

Similarly, putting all individuals of one ethnicity or religion in a category labelled "dangerous" may in fact undermine identification with the larger community and encourage radicalisation.

As systematic surveillance and the capacity for data retention and analysis expand, an alternative to profiling may emerge.

Rather than targeting a specific group for closer examination, it may be possible to gather information on the entire population in such depth that human intervention - with the subjectivity and potential for bias that this brings - is significantly reduced.

Bias may still affect the manner in which data is organised and analysis prioritised, but it should at least be more evident than the personal choices of individual analysts. It will leave a trail - and the possibility of accountability.

Privacy and secrecy

MR EDWARD Shils, a sociologist writing soon after the McCarthy hearings had shaken the US half a century ago, argued that liberal democracy depended on protecting privacy for individuals and denying it to government.

The following decades have seen precisely the opposite happen: Individual privacy has been eviscerated while governments have become ever more secretive. This trend increased under the Bush administration after Sept 11 and, if anything, has accelerated under President Barack Obama.

Singapore - which lacks a right to privacy and freedom of information laws - has gone further still.

In such an environment, it seems naive to seek a "balance" between liberty and security.

Far better to be clear about who has access to the data that is already being collected, and to have a little transparency for the coming debate about how this data is to be used.

stopinion@sph.com.sg

The writer is the dean of the National University of Singapore's Faculty of Law. His most recent book is One Nation Under Surveillance: A New Social Contract To Defend Freedom Without Sacrificing Liberty, which was released in paperback in April.

By Invitation features expert views from opinion leaders in the region and Singapore.