Strengthening standards for cybersecurity and surveillance

Surveillance is a vital tool in the fight against terrorism and organised crime, but governments must do more to convince the public of its necessity

By John Lyons, chief executive, International Cyber Security Protection Alliance

In the wake of Edward Snowden's revelations, a great deal has been said, mainly by politicians in the United States, about what steps will be taken to ensure that citizens' privacy is respected. There have been embarrassments too at ministerial level, about the US and UK intelligence agencies 'spying' on their allies and friends – something that, apparently, they have been doing for years.

Security, intelligence and law enforcement agencies have complained about the disastrous effects the publication of these national secrets could have on their ability to fight terrorism and organised crime.

So how does the international community expect to address these issues of security and privacy? These two often conflicting requirements are fundamental rights that are vitally important to all. Yet few governments will be likely to address the issues at all, leaving the G7 members to draw up their own doctrines governing future national communications surveillance activities.

Along the way to doing so, it is helpful to understand the context in which such operations are carried out. To do this thoroughly and honestly, and keep citizens engaged and win their support, governments need to be much more open about the necessity for such surveillance. This failure to communicate to citizens the proportionality and necessity argument is one of the clearest lessons learnt from the Snowden fiasco.

Systemic failures

According to Oxford Dictionaries, the definition of a fiasco is "a complete failure, especially a ludicrous or humiliating one". That precisely describes the Snowden affair. All organisations that hold highly sensitive information, be they in the government sector or in industry, would do well to consider how it is that one person in a relatively junior role could gain access to significant amounts of critically important information. It happened before in the US in the case of Private Bradley Manning. To have it repeated so soon with Snowden – a contractor at the US National Security Agency – suggests that there are systemic failures in the way in which very important information is stored and accessed. Lessons are clearly not being learnt and remedial measures not being implemented quickly enough.

It is self-evident why this is important to the future integrity of information held by governments and companies. However, one of the less attractive, and possibly equally damaging in the long term, by-products of these revelations is their impact on citizens' trust in their governments and security agencies. This growing lack of confidence in governments' ability to secure important information will have detrimental knock-on effects on many areas of daily life.

Policies relating to, for example, the need for doctors and hospitals to share medical information nationally will struggle to gain acceptance by patients and many of their doctors. When governments fail to secure information from unauthorised access, or to safeguard information when it is in the hands of those who require it, they do themselves and every citizen a disservice.

Transparency: vital for gaining public support

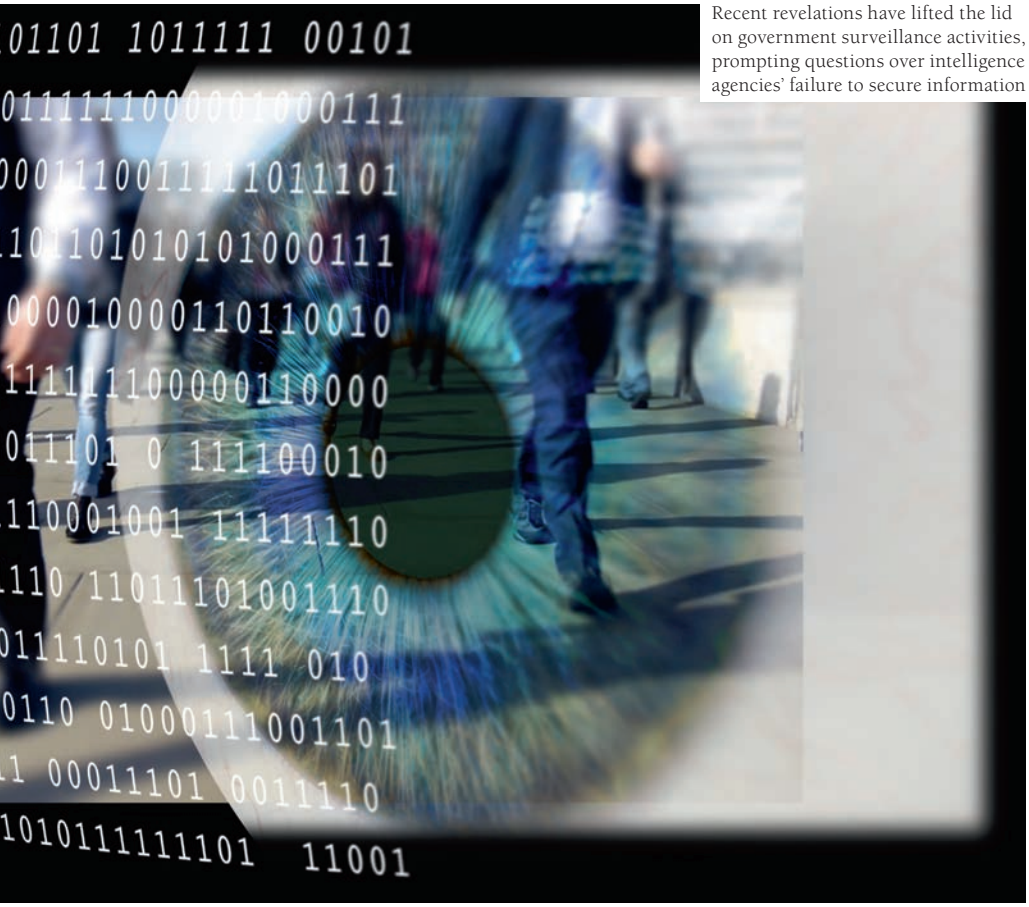
First and foremost, governments that carry out communications surveillance with the aim of protecting the lives of citizens and preventing harm must embark upon a public information awareness campaign that supports these activities. This can be achieved without revealing techniques or secrets about government capability; however, methods have to be invented because it is imperative to keep secrets between those who 'need to know' what they are.

PETERHOWELL/ISTOCKPHOTO

(Of course, not all governments carry out this work for these reasons. There are many that conduct this type of surveillance for the purpose of identifying those who disagree with them in order to incarcerate them. This article is not concerned with such regimes.)

These are some of the arguments that could be put forward to form the basis of an awareness campaign directed at citizens:

- Communications surveillance is carried out by security and law enforcement agencies only to save lives and reduce harm to citizens.
- Such operations are necessary and proportionate to counterterrorist



Recent revelations have lifted the lid on government surveillance activities, prompting questions over intelligence agencies' failure to secure information

Governments that carry out surveillance with the aim of protecting the lives of citizens must embark upon a public information awareness campaign that supports these activities

operations and in the fight against organised crime. Sometimes, individuals who carry out criminal acts will also be the subject of surveillance activities.

- All operations are authorised at ministerial level and overseen by an independent organisation that reports to parliament and identifies inappropriate activity.
- Terrorists and organised criminals are using very sophisticated applications available on the internet, mobile devices, computers and phones to support their illegal operations and to cause harm to innocent people at home and in other countries.
- In order to identify this criminal activity and the people engaged in it, it may be necessary to conduct surveillance of 'innocent' communications by citizens who are not engaged in criminal activity. Authorities will work hard to ensure that this information is discarded as quickly as possible. They do not need it and they want to concentrate their activities on identifying, disrupting and, wherever possible, bringing to justice those who would seek to inflict harm on others.

Examples of successful operations that have been brought to court could be highlighted without the need to reveal techniques. Blogs and Q&A sessions could also be created to answer the public's questions. The media should be engaged in the campaign, and ministers should speak about these activities and hold public debates about them. This level of engagement should be continuous and not reactive.

'Blue-on-blue' surveillance

Some might be forgiven for thinking that government security agencies should have enough to do by surveilling countries that are potentially hostile. What hope is there for international accord and for building lasting trust among countries already party to treaties such as NATO's if a government cannot be sure that its allies are not spying on it?

Countries need assurances that this trust, hard won and easily lost, is not jeopardised by security and intelligence activities carried out on the basis of some outdated doctrine.

On the other hand, it could be argued that governments ought to be better able to protect their communications and information against threats from any quarter. This is axiomatic, but it should nevertheless become the norm that one does not spy on one's friends. Perhaps, it would be more helpful instead to alert them to weaknesses in their systems and help repair these, rather than use them to infiltrate government systems.

It is difficult for governments to justify seeking to discipline those who have illegally gained access to their systems while at the same time conducting surveillance of other governments' systems. In the interests of international harmony and to encourage the sharing of vital intelligence among countries that are already members of a club, they should at least consider signing up to an agreement that outlaws surveillance on each other. Security and intelligence agencies can then get on with the job of conducting communications surveillance on hostile countries and on those who would bring death and destruction to the streets. ■