PRISM schism: the NSA leaks reveal a broken system

If reports are to be believed, the US National Security Agency (NSA) has had “direct access” to systems run by Google, Facebook, Yahoo and Apple. While all the companies named have used similar words to deny those claims, the alleged scale of the surveillance, its sophistication and the lack of independent oversight are still very alarming.

All of the above points to a worrying breakdown in procedures that have been around for decades – for good reason – in the area of lawful interception.

Most countries have some form of legislation governing lawful interception of communications. If an organisation offers some form of publicly-available communications service, it may be obliged to deliver the content of communications or information about that communication to the relevant law enforcement or intelligence agency.

Such legislation covers not only telecommunications companies, but Internet Service Providers (ISPs), Application Service Providers (businesses that offer software services to customers) and social-media sites. If a publicly-available service can be used for communications then, in most cases, it can be subject to interception obligations.

Interception

In the US, as in most Western countries with a strong rule of law, lawful interception usually has strong controls to ensure it’s not abused; this usually entails some form of judicial oversight whereby a warrant for interception is issued by court order.

The warrant is then served on the communications service provider who delivers those communications specified in the warrant to the law-enforcement agency.

A video grab courtesy of The Guardian newspaper showing former CIA employee Edward Snowden during an exclusive interview. Guardian/Glenn Greenwald/Laura Poitras/EPA

By having a separation of responsibilities whereby the communications service provider carries out the intercept at the request of the court there is an auditable separation of responsibilities that helps ensure interception capabilities are not abused. There is no direct access by the law enforcement agency to the data.

It has to be said, though, that since 9/11 the US controls governing lawful interception have been loosened, notably in the area of metadata collection. Metadata is information about a communication between parties rather than the content of that communication, and is typically used in carrying out network analysis of who is connected to whom.

Metadata associated with an email would consist of the sender and the receiver of the email. Using such information, a map can be built showing the relationship “networks” of people of interest. Other information, such as location, can also be integrated into network maps.

Often metadata is more useful than the content of communications. A phone call pattern to, say, a psychologist, followed by a call to a suicide hotline, provides plenty of information, and can be computed, coded and stored quickly and easily.

In the US, under the Patriot Act, enacted after the 9/11 attacks, it was unnecessary for a warrant to be issued before metadata could be collected.

Shining light on PRISM
You probably know by now that the latest revelations concern a system referred to by the NSA as PRISM. If the claims by ex-CIA employee Edward Snowden are to be believed, PRISM takes feeds from telecommunications companies and social media and integrates them to produce usable intelligence.

There are a number of issues of concern here:

Perhaps the most worrying is the arbitrariness of data collection. Intercepts are usually understood to be specific to particular organisations or individuals. Information is targeted to those of interest.

The leaked slides suggest data is collected somewhat arbitrarily based on keywords or location.

The second concern is the reference to

| Collection directly from servers of […] Microsoft, Yahoo, Google, Facebook … |

If “direct” means the intelligence agency is able to collect data without judicial oversight, this represents a serious breakdown of the separation of responsibilities necessary to reduce the risk of abuse of this technology.

Representatives of the companies involved have claimed the NSA does not have direct access to their servers, but this begs the question of what information they do, then, have access to.

Twitter

Facebook

The third concern is that one of the slides lists a large variety of content that analysts will have access to. Content collection, as opposed to metadata collection, has previously been very tightly regulated. It is alarming that this might no longer be the case.

Lawful interception is a fact of life. Law enforcement agencies have been intercepting communications almost as long as there have been communications technologies.

But if abuses are to be avoided it’s important such interceptions remain tightly regulated.