Submission No 103

Inquiry into potential reforms of National Security Legislation

Organisation: Earthwave Corporation

Parliamentary Joint Committee on Intelligence and Security

Response from earthwave to Government request for submissions regarding "Equipping Australia Against Emerging Threats" (Deadline August 20, 2012)

As a provider of security services to "custodians of critical infrastructure" including a number of notable energy providers, earthwave appreciates that governance, information and intelligence sharing could significantly improve the security posture and reduce the likelihood of falling victim to an as yet unseen threat to resilience and ability to continue to deliver power to the grid in the face of a cybersecurity attack.

That said, earthwave strongly believes the path to true cybersecurity need not unduly infringe on personal liberty and privacy. As data storage capacity grows ever greater and cheaper, the risks of wholesale surveillance and storage of vast amounts of video and audio data will increase and needs to be acknowledged.

Recently, an electrical engineer at UCLA and a senior fellow at the Brookings Institution in the U.S., John Villasenor, was reported by The New York Times to estimate "that to store the audio from telephone calls made by an average person in the course of a year would require about 3.3 gigabytes and cost just 17 cents to store, a price that is expected to fall to 2 cents by 2015. Tracking a person's movements for a year, collected from their cellphone, would take so little space as to carry a trivial cost. Storing video takes far more space, but the price is dropping so steadily that storing millions of hours of material will not be a problem soon."

The temptation for governments and other large organisations might be to treat cybersecurity in a passive way, simply collecting vast amounts of personal data and believing security rests in having quantity not quality. In addition to the issue of privacy, this approach might also lead to neglecting the two pillars of holistic cybersecurity: detection and response. This would only weaken, not strengthen, our security. The best kind of cybersecurity is built around vigilance and vigilance is powered by intelligent monitoring, not mere accumulation.

We still need to accumulate as much information as possible so we have the necessary information to interrogate in event of a security threat. However this accumulation of data does not necessarily create a risk to an individual's privacy as it is only when something or someone fits a certain pattern that deeper analysis of their personal data will ensue.

As proponents of wide surveillance, we think the requests of law enforcement agencies do not go far enough! They appear to have limited their requests for what they think they can realistically secure (such as meta data) for fear of coming away with nothing. Lobbying by the very people who may pose a risk appears to have worked.

From a practitioner's perspective you should not get side-tracked by what is possible to know, and instead focus on what *needs* to be known. Once the practitioner has worked that out, they should declare it to all and then create the right detection and response strategies to deal with the threat. This should not infringe on the privacy of any law abider.

If there are then drivers/indicators to dig deeper, investigators should then be able to gain the authority to explore everything that it is possible to know in relation to the investigation. Why would anyone deny authorised investigators this access?

For example, in the enterprise environment, deep packet inspection technologies record and replay all traffic including the viewing of all documents transmitted and all voice conversations made over

IP networks (VoIP). In the event of something going wrong investigators are then able to follow the trail to find what, when, where, who, how and perhaps why the event occurred.

Timely detection and response can prevent or mitigate loss, but the ability to go back in time to understand everything about what lead up to that alert condition would provide evidence for prosecution and more importantly help identify “markers” for even earlier identification of a similar situation, and deliver “predictive intelligence” to allow the prevention or significant reduction in the risk of the condition arising.

Complete data capture and analysis should be regarded as critical research for developing detection and response efficiencies and reducing risk.