The Next Cyber Security Threat: Export Controls

The debate around cybersecurity tools and terrorists has been raging between government entities (US and non-US) and the computer industry for the last couple of years. The debate came to a head when a proposed rule was published in the USA federal register in 2015 that would introduce export controls on cybersecurity items and research. These have since been made official not only in the USA but also in Australia.

YOU ARE INVITED TO PARTICIPATE in a (free) workshop debate on how the Australian cyber security R&D community can be appropriately represented in future decisions by government on issues that affect our work, business and research.

WHEN: Monday July 4, 2016 from 3p.m. to 5p.m.

WHERE: Deakin University's Corporate Offices
550 Bourke St., level 3, Melbourne CBD
Ask for the ACISP Export Controls workshop room

AGENDA: 3:15. Tea/coffee/water/snacks in the open area adjacent to the room.

3:30. Brief ppt background by Prof. Lynn Batten, Deakin University

3:40-5p.m. A panel discussion/round table with Melbourne lawyer ***Helaine Leggatt*** (Helaine specializes in IT law and was an invited speaker at Asiacrypt in Taiwan), Dr. ***Vanessa Teague***, Melbourne University, Prof. ***Ed Dawson***, Qld Univ Tech., and ***Damien Manuel***, National Branch Director, Australian Information Security Assoc.

5:05-6p.m. Steering Committee Meeting for ACISP attendees.

6 - 7p.m. ACISP welcome reception

The cybersecurity control debates are not new. They have been around since the early 90's, when the computer industry began the task of trying to move encryption technology controls from the **International Traffic in Arms Regulations** (ITAR) to the Commerce Control List (CCL). Movement of encryption technology from ITAR to CCL represented a relaxation of controls for products with embedded encryption technology. Up until that point encryption was viewed as a tool used only by governments. The act of moving encryption technology was perhaps the biggest factor in the explosive growth of the Internet. Today, encryption is a necessity for the protection of everything we do – from buying an item on the Internet to downloading purchased music or books, to protecting our bank transactions. In short, encryption has become ubiquitous. The major concern with encryption is that it can be used by terrorists and criminals to hide their plans and activities. Last year, the encryption debate expanded to include cybersecurity tools. (https://www.netiq.com/communities/cool-solutions/netiq-views/the-next-cyber-security-threat-export-controls/)