From: Len Spyker
To: Assistance Bill Consultation
Subject: Encryption laws
Date: Thursday, 6 September 2018 10:38:04 PM

Preamble:
I apologise that some web sites have mangled my earlier attempts to send comments.
Please ignore my earlier fragments in the same name,
I hope this goes through intact:

Re: Encryption laws.

Good safe encryption is necessary at all levels for a society to function properly

The only feasible way to go on laws of controlling encryption is to have global UN +ISO mandated legal levels of encryption.

My modest proposal is to have well defined global UN +ISO levels of encryption that can be made into usable laws

Level 0 Personal communications emails and non-encrypted attachments

Level 1 Banking on-line e-mails and level 0 en-encrypted attachments

Level 1 Religious orders, charities and NGO e-mails and level 0 un-encrypted attachments

Level 2 Industry IP, patents, CAD, contracts and drawings + level 0+1 encrypted attachments

Level 2 Banking Interbank transfers SWIFT++, Bank Databases, + level 0+1 encrypted attachments

Level 3 Governments Matters of State, Databases, + level 0+1+2 encrypted attachments

Level 3 Military Weapon systems, Battle plans + orders + Databases,

Plus level 0+1+2+3 en-encrypted attachments

WARNING:

The history of placing “secret back doors” into computer based systems has been often tried and has failed time after time. One security disaster after security disaster.

Often the “enemy” found out rather quickly how to use the same (now unstoppable) back door against the very people who created this idiotic monster in the first place.

Especially when the “back door” creators were stupid enough to use the same (unstoppable unblockable) hardware back door in their own massive security equipment!

Most current and ancient encryption systems hardware or software has been found to have fundamental flaws (accidental and yes even some were planned to have special flaws for use by the creators).

Some encryption algorithms contain software “backdoors” (unstoppable unblockable) that have made them crack able in minutes and not taking centuries as predicted.

Note carefully: In this world there are no 100% secure computer systems, period. True - ask some real experts and not your local IT guy.

Anybody who says otherwise are just pig ignorant living in la-la land or IT sales people

Even the NSA got hacked into from outside the USA. Then their own “secret” tools and intelligence weapons were used against them.

100's of millions of our own credit cards some with our privacy details are for sale of the black web.

Every Australian government computer has known backdoors and future unknown backdoors and

flaws in both the Intel and AMD chips and all the governments Cisco routers. J

Just ask your own SAS experts.

Note carefully: There are no proven secure OS software Operating systems.

Conclusion:

Needless ill-conceived laws and dilatant meddling in security and encryption by the ignorant and misled willful will destroy Australia society instead of helping become a better safe secure place

Len Spyker

[redacted]

[redacted]

[redacted]