Child Protection (Offender Reporting and Offender Prohibition Order) and Other Legislation Amendment Bill 2022

Submission No:	1
Submitted by:	Robert Heron
Publication:	
Attachments:	No attachment
Submitter Comments:	

From: [redacted]
Sent: Thursday, 3 November 2022 1:50 PM
To: Community Support and Services Committee
Subject: Sub 1 Child Protection (Offender Reporting and Offender Prohibition Order) and Other Legislation Amendment Bill 2022

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Submission, Child Protection (Offender Reporting and Offender Prohibition Order, Child

To the committee,

I see that some of you have just learnt about Layer 2 networking. Welcome to the horrific world of I.T. I would suggest legislation adopt Layer 1 terminology rather than specific abstract protocols. MAC addresses are always software defined -firmware is an artificial distinction- and the user familiar only with the operation of a device at the application layer or OSI 7/+ -human machine interface engineers expand the OSI model indefinitely- won't realize this. Are you providing technical experts to facilitate compliance or is compliance entirely the burden of those subject to the reporting requirement? It is not completely clear. Virtual interfaces can indefinitely enumerate MAC addresses associated with a device such that reporting a MAC address of a device could serve no purpose. It is possible for a device to roll the MAC between 00:00:00:00:00:00 and FF:FF:FF:FF:FF:FF and all values in between or simultaneously use all values. A MAC address is not a hard-coded unique identifier. Modern systems still label partitions or default configurations as EPROM data but is often an abstraction and OTP MAC addresses are no longer the norm. To be safe, the affected persons would need to report all possible values for every device. This is a misunderstanding of the Open Systems Interconnection model.

Clause 42 makes no sense. What does,"physical address, wireless ID or wi-fi address" mean? This would be a BSSID, ESSID or tautologically a MAC address? The bill needs consultation with technical experts. They will probably explain side channel attacks, user fingerprinting and herd analysis that renders physical reporting unnecessary. It may not be legal to require such reporting if alternatives exist and compliance becomes punitive. For example companies could start concealing the MAC addresses on fleet vehicles and the unique reporting requirement is matchable that has a foreseeable punitive effect that they have not been sentenced to.

Clause 22 is a mistake. Being the keen student of embedded design and having remained pure and true to my first loves -C89 and assembly- let me explain how terrifying IoT is. Smart devices aren't custom built. That is marketing. The production cycle for consumer smart devices is short. Developers use SDKs and reference designs. They code in intellectually repulsive languages with *garbage collectors* like python and java. They take an off the shelf design and use an off the shelf code examples to build a system. This accelerates the design process. The SoCs are just a CPU with some logic glued on for specialized tasks like network, audio and video processing. Similarly, the smart TV is just a regular TV with a mobile phone glued inside. The smart fridge is just a regular fridge with a mobile phone glued to the door. It seems complicated but it's all so abstract that in theory one simply has an idea, collects some standardized modules together, purchases the IP block volume licensing, 3D prints a case then sells the commodified intellectual property as a new gizmo. It's especially not hard when they don't bother to configure the software properly and just patch together a bunch of sample configurations and leave user non-configurable services running.

Intellectual property firms have gone one step further with server side data processing so that people buy a "smart device" that only has just enough processing power to record and transmit all of your conversations to an overseas data hub for processing, thus protecting their intellectual property by preventing customers from actually possessing the smart device. The way this is implemented is very different from Wyse and DIGITAL's original zero/thin client models. Due to the very poorly performing code used in these devices they require substantial computational resources to barely manage to perform the most simple of tasks. These devices are fully functional computers and distributed transaction devices. Many of them contain identical or superior hardware compared with embedded industrial terminals.

This new form of obscenity requires a new discipline of research for a new era -forensic teledildonics. Technologically facilitated sex crimes. These are examples of penetration testing. This is a very scientific digital forensic procedure like hitting your door knob with a hammer to see if it falls off. Software defined radio for intercepting unencrypted sub-GHz transmissions from baby monitors.1 The infamous HAPPYCOW/HAPPYCOW Hackable RC car with cameras that tilt all the way up that is actually built around configurable router hardware.2 And then there is Kodi. This is technically a piracy enabling app that can easily be installed on set top boxes or smart devices but the way it works is that the user subscribes to private trackers and usenet indexes -private file servers and search engines- ostensibly to illegally download television shows. There are many guides online for setting this up with Radarr, Jackett, Debrid, NZB etc. in such a way that it behaves at the application layer exactly like an automatic video caching streaming service. These programs don't host the content, they just bring it all up to the application layer. an easily configurable human machine interface that automatically serves the user illegal content. The content gets de-identified and uploaded across multiple legitimate file servers. I have no proof and it would be foolish to go looking but I suspect beneath the prime time content there is alternative even more illegal content that is a distortion of the streaming model. It's enough to convert any parent to Waldorf-Steiner. So in regards to checking if the fridge is running stock firmware then no it would be inadvisable to specifically exclude the fridge in legislation and a trivial exercise even for a child to copy whatever flash module is in use for analysis. It's not military cypher boards that have multiple layers of self-destructing anti-interference devices, they make test clips that just slip over memory chips. I understand that seems a bit like some mission impossible fiction but that's how they are rapidly programmed in a factory assembly line.

1. Aubin, D. Patterns of Life: Investigating rtl-sdr2832U. Carleton University: Comp4905 Honors Project. http://service.scs.carleton.ca/sites/default/files/honours_projects/2015/Honours_Project_0.pdf

2. Cooper, M. February 5, 2015. Hacking the WiFi Spy Tank. Kogan Dev Blog.

https://devblog.kogan.com/blog/hacking-the-wifi-spy-tank

Robert Heron
[redacted]