We, The People, Are NOT the Enemy!

by claire *Sunday, Apr 23 2017, 10:07pm*
international / prose / post

> Western populations have allowed various western states to implement PAN-surveillance, which means EVERYONE! The excuse for such was that it 'keeps us safe,' whereas studies/FACTS reveal that terrorist attacks are not impeded by pan-surveillance -- in other words pan-surveillance is NOT a preventative measure; however, it does offer itself to a multitude of uses particularly for the corporate community, which are able to source these databases to sell advertising more effectively. It also lends itself to the most intrusive form of personal privacy breaches, which values and liberties our forefathers fought world wars to preserve.

Former NSW Premier, Mike Baird, knows more about the Sydney siege than he would care to Reveal

Personal data including meta-data is now stored without majority approval for a number of years revealing our habits likes dislikes and moods -- computer algorithms are easily able to mine and determine reams of personal details that most honest citizens would rather keep to themselves, notwithstanding the fact that the majority of people REMAIN opposed to these outrageous intrusions which continue and become more intrusive by the day; yet the majority are not criminals or warrant this type of surveillance and profiling -- the iPhone for instance, touts its security features as a major sales feature, however, it is simple with the appropriate tools to hack these devices, especially by various government agencies, which have no business hacking the phones of private, honest citizens. Now, you may have been led to believe that if you have nothing to hide you have nothing to worry about; this feeble excuse, as that is all it is, has not prevented various professionals and citizens coming to the attention of nefarious regulatory agencies because their names are scantly similar to known criminals. Solicitors have been put on 'no fly' lists as a result, without explanation or recourse to have their names removed from 'hot' lists.

It is easily appreciated that once these automated computer mechanisms do their INACCURATE dirty work, human staff in various professions (e.g. airports, finance, etc) become too frightened to pursue these matters and so abide by the inaccurate data or flaws in the system, which causes huge grief for innocent victims. And regardless of what you are told, like, 'your record has now been corrected,' we know from decades of experience that the 'hot' aspect is only removed from viewing on a superficial level, the 'hot' aspect remains though hidden from most, as regulators, most of

which staff have no technical background, are loath to remove such as they never question the policies or implementations of their employers, notwithstanding they fear for their jobs.

Of course few citizens oppose the targeted surveillance of known criminals, which felonious information is determined by operational procedures or basic policing work. Most would agree that these types should be monitored by regulatory authorities, however, in Australia, a known unstable criminal with terrorist tendencies who was monitored by NUMEROUS government agencies and state police, was mysteriously taken off watch by all these agencies a few weeks before he committed an entirely avoidable terrorist attack on citizens, which resulted in two hostage deaths. This entirely avoidable event is now known as the *Martin Place Siege*. So where is the effectiveness of pan-surveillance and the appalling failure by agencies that scream we must maintain pan-surveillance? Their failures are tragic and gross, whereas targeted police work resulted in the 70's -- prior to the technological era -- in the apprehension of Croatian fascist extremists training in the bush with weapons and other devices to attack various targets -- this group had been responsible for numerous bombings in the Sydney CBD and other locations targeting THEIR 'perceived' enemies, most of whom were honest law abiding citizens.

It becomes apparent that not only are surveillance systems flawed today but policing is far too reliant on these methods which has resulted in very lazy and unskilled (in basic intelligence gathering operations) police and Intel agencies, as the 'Martin Place Siege' emphatically PROVES, though the government coroner did not venture into this realm for obvious reasons.

Enough information has been provided above to prove the point though plenty more information exists which reveals the failure of pan-surveillance to prevent crime. Therefore, populations world-wide that are unjustifiably subject to pan-surveillance should remove all governments that support it and replace them with representatives that support targeted surveillance ONLY. This is a vote winning issue for politicians that have the public's interest foremost on their political agendas.

Pan-surveillance and pan meta-data storage are not only privacy outrages, studies have proven that pan-surveillance does NOT prevent crime, however, basic police/detective work remains the most effective means of identifying and apprehending criminals and ensuring the safety of the community at large.

The following video leaves no doubt about the matter:

> **iPhones/smartphones = iSpies**
> by Roqayah Chamseddine
>
> Most of us carry smartphones and watch web-enabled TVs without much thought. But the revelations found in Wikileaks' "Vault 7" release warn that we should consider the sinister capabilities that such devices could lend to those who might abuse them.
>
> Since its launch in 2006, Wikileaks has reportedly released over 10 million documents, including controversial disclosures that have helped unravel war crimes, uncover corporate secrets and even brought to light explosive revelations stemming from Hillary Clinton's most recent presidential run.
>
> Despite facing widespread international denunciation, Wikileaks has remained faithful in blowing the whistle on information that would have remained hidden from the public. These secrets have helped to expose many layers of the global state security apparatus and aided in shaping the discourse surrounding government and corporate

transparency.

On April 7, Wikileaks released 27 documents from the CIA's Grasshopper framework, a platform used by the agency to infect electronic devices such as phones, computers, and televisions for surveillance purposes. This information dump was part of a series known as "Vault 7," which targets the agency's covert hacking program. "This extraordinary collection," Wikileaks writes, "which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA."

According to the documents provided by Wikileaks, knowledge of the CIA's invasive surveillance tools wasn't confined to the agency, or even the National Security Agency. In fact, the details of these exploits were bought and shared by Britain's Government Communications Headquarters, as well as other intelligence agencies.

So what tools does the CIA have in its surveillance arsenal? Over 8,000 documents found in the "Vault 7" series reveal weaponized malware, trojans and viruses that could be used to spy on both domestic and foreign entities, impacting a variety of seemingly harmless household devices. Apple iPhones, Windows PCs and even Samsung TV sets can be used to conduct surveillance on anyone the CIA chooses to spy on. For example, one program named "Weeping Angel" details methods that can be used to hijack a Samsung F8000 TV in order to make it appear to be off when it is actually powered on.

The claim that your TV could be used to spy on you is no longer one of conspiracy. It is now our reality. "By hiding these security flaws from manufacturers like Apple and Google, the CIA ensures that it can hack everyone, at the expense of leaving everyone hackable," WikiLeaks says. And these, by all accounts, are just the tip of the iceberg.

The "Vault 7" series, which has been described as being the largest leak of its kind targeting the CIA, originated from an "isolated, high-security network" within the CIA's Center for Cyber Intelligence. The documents it contains were revealed to Wikileaks by way of an undisclosed source, though they've noted that their source could be a former U.S. government hacker or CIA contractor.

After the "Vault 7" series was first published, Trump administration spokesman Sean Spicer revealed the White House was concerned, and that "[a]nybody who leaks classified information will be held to the highest degree of law." Despite these threats, WikiLeaks continues to release classified documents, showing us at least some of the secrets behind the CIA's curtain.

[People should also note that hacking -- regardless of perpetrator -- remains illegal under various communications laws in all western nations. The current outrageous situation is easily dealt with by existing LAWS and social/political will.]

http://www.mintpressnews.com/video-iphones-ispies-wikileaks-vault-7-revelations-continue-terrify/227066/