Big Data meets Big Fridge (a frolic)

Edouard Estaunié
West Melbourne Institute

Summary: This article offers a possibly optimistic view of the influence of the new anti-terror laws on the profitability of the telecommunications industry.

"Looking back, the 2010s were the decade in which Big Data took off and telco shares went through the roof.

"And with hindsight from year 2020, heh heh, we can see that the main cause was Big Government.

"It wasn't just the endless traffic from the bots set up by all those charming politicians to erase their broken election promises in Wikipedia and the media websites, under their Right to be Forgotten laws. Or the counter-traffic from the bots set up by concerned members of the Historical Societies, to redeploy the video clips of the same pollies caught making those promises *in flagrante delicto*.

"Nor was it just the endless downloading of Hollywood and indy films dealing with imagined dystopias in the near future (*Matrix*, *The Road, Cloud Atlas*, *The Hunger Games*, …), which resonated amongst first world citizens, so totally frustrated with living in supposed democracies that seemed to be trending towards police states.

"No, the major source of data traffic was the provenance of Big Spook – the government security agencies that blossomed under massive funding increases through the post-9/11 and counter-ISIS anti-terrorist legislation. Much like the CIA had grown huge and out of control during the Cold War – and again under Bush.

"In the early days, Big Spook was happy to connect to the telcos' backbone routes, copying and recording zettabytes of traffic for their data-mining software.

"But once they got deeply interested in profiling potential terrorists, and kept persuading the pollies to broaden the definition of 'terrorist' so as to improve their performance results, the

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.74

passive detection of incriminating data via the Internet became … inadequate. Especially when Electronic Frontier and other Internet libertarians began producing effective tunnelling software to evade Big Spook's best anti-encryption tools. Hah!

"To profile their suspects, Big Spook needed more data than the oceans of it being sucked out of the burgeoning public WiFi systems. It saw great potential in profiling personality types from eating and imbibing habits. Animal liberationists, for example, were almost universally vegans. Islamic jihadists would demand halal meat. Bikie gangs would favour cocaine, ice and other drugs. And so on.

"From 2016 the remotely controlled fridge became a best seller amongst consumers, and simultaneously the target of Big Spook. To monitor the fridge contents it would need to mimic signal traffic from the owners' mobile devices, and divert the fridges' responses to its own portals. Easy peasy. As was hacking e-health records from a variety of sources (hospitals, GP surgeries), and lifting shopping records from retailers – a routine exercise. And snooping the web-cameras in home and office security systems: the biggest generator of 'black ops' traffic.

"To disguise its cowboy surveillance operations, Big Spook would set up and pay bogus accounts with major telcos. Big Spook of course has vast, secret budgets beyond any official oversight.

"And thus the projected traffic from the known Internet of Things has exceeded the analysts' forecasts, year after year.

"No-one has lost money investing in telco shares during the past decade, my friends."

References

News.com.au. 2014. 'Anti-terror laws pass Senate, giving Australia's ASIO spies increased power and protection', 26 September 2014, at *http://www.news.com.au/national/antiterror-laws-pass-senate-giving-australias-asio-spies-increased-power-and-protection/story-fncynjr2-1227071099923*

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.74