Apathy Let Cambridge Analytica Abuse 50 million Facebook Accounts

written by Peter Clausi | March 24, 2018

It was revealed last week that Cambridge Analytica abused personal information from 50 million Facebook accounts in early 2014 to build a system to profile individual American voters for the 2016 presidential election. The goal was to then target the users with personalised political advertisements attacking Hilary Clinton and loving The Donald. It's still not clear whether this was illegal or merely repugnant.

Most people are focussing on the fact that Cambridge Analytica was headed at the time by Steve Bannon, which provides yet another malodorous link to Trump. Facebook's share price is down about 12% but so far there has been no accountability apart from the inevitable class action litigation lawyers circling. What matters the most here is that we are becoming de-sensitized to data breaches like this.

$300M of Etherium permanently lost. Hey, it's just crypto and it wasn't mine, so who cares?

Do you know anyone who lost sleep over 143 million Americans and 100,000 Canadians that were exposed by Equifax's massive data breach.

Every Yahoo account was compromised in 2013, which Yahoo did not figure out until 2017. That was 3 billion accounts. You likely had one of those accounts. Did you complain about it?

Citibank failed to protect the personal data (including birthdates and Social Security numbers) of approximately 146,000

customers who filed for bankruptcy between 2007 and 2011. That's adding insult to injury.

40 million Target customers were exposed in 2013. The remedial cost to Target, not including the class action litigation, was roughly $252M. Did you join the class to get your rightful piece of the settlement?

$81 million stolen from the Bank of Bangladesh by compromising the Swift system in 2016. This was the second time Swift was used as a medium of theft. But hey, that could never happen over here in the civilized world, right?

Look at the lists here and here and here for some of the largest data breaches of all time. How many of these do you remember, or care about?

Even worse, according to the Online Trust Alliance in its terrifying *Cybersecurity and Breach Trends Report* from January of this year, is that 93% of these breaches were self-inflicted and easily preventable. Apathy is our real enemy.

And next up are the assaults from Artificial Intelligence.

AI spans a broad area. A Nest WiFi-enabled thermostat can self-regulate if it feels the sun directly on it rather than air in the home environment – is that 'intelligent' or just good programming? Cruise control on your car? A video game that gets harder the further you go and that learns your favourite moves? Neural networks? Deep learning? The hated robo-advisor? Predictive weather analysis? Smart tokens in the ICO universe?

AI is just a software operating in a hardware environment, but somehow it has gained noble status. Perhaps it's the use of the word "intelligence" that lulls us into thinking that the software is actually alive.

It’s not. It’s just software, a compendium of zeros and ones that open and close circuits inside chips. Software is vulnerable to coding errors, intentional or negligent. It’s vulnerable to breakdowns in its hardware. And it’s entirely vulnerable to malicious third parties for cryptojacking.

Our courts and insurers will have to address who becomes liable when those things go wrong. The worse situation is where software causes death, like earlier this week when a self-driving car killed a woman in Tempe, Arizona. Elaine Herzberg was walking her bicycle when she was hit by a vehicle in autonomous mode going 40 km/h. It doesn’t take a crystal ball to see Mr. Herzberg is the first of many such deaths.

Who will carry the financial burden of the error when smart tokens co-ordinate a contract for one billion rolls of toilet paper when the intention was for 100 rolls of paper towel? Is this contract law or negligence? Can you contract out of liability? Medical diagnostic software misses an obvious cause resulting in patient death? Who pays the repair bills when Skynet finally goes live and the Terminator kicks in your door?

Vernor Vinge’s 1993 short paper *The Coming Tehnological Singularity* is a marvel of literature that manages to inspire and terrify at the same time. Should something we created actually develop its own intelligence, the pace at which technology would from that point develop would be inconceivable to humans. The human era would be over.

Back to the breaches, both malicious and self-inflicted. Incompetence and thievery have been with humanity for recorded history. The first trojan horse was the serpent surreptitiously attacking the Old Testament God by way of his human creations and an apple. Sadly, we do need various levels of government to help us defend ourselves. This will require some levels of

regulation, even if unwanted.

The CryptoCrowd may not like it, but regulation is needed and it's coming. At least there seems to be some regulatory recognition that data is a different world requiring a different set of regulatory parameters. See for example the British Columbia Securities Commission's 2018 outreach efforts seeking innovation while maintaining confidence in the capital markets.

This apathy is a strange mindset, especially since the business world otherwise takes confidentiality seriously. We sign confidentiality agreements and NDA's. We expect our employees to leave our IP at the office. Securities laws exist to prevent insider trading and to protect the dignity of the market. Larger boards have committees specializing in privacy and data protection. There are few things more valuable to any company than the integrity of its data.

So we should be outraged by these ongoing assaults on us, our data and our companies. We should be in the streets, with torches and pitchforks, demanding that heads roll and attackers be found. Instead, we shrug and say "What can we do? I'm just one helpless person. The government will protect us." That only goes so far.

We have to use what the government gives us. CASL (Canada's AntiSpam Legislation) is a horribly mis-named piece of legislation that has teeth. It codifies an individual's right to control the inbox. It isn't about spam, it's about your digital liberty.

The GDPR is the European Union's approach, and it's a good one. A prior article explaining GDPR is here. Recent recommendations from House of Commons Standing Committee on Access to Information, Privacy and Ethics indicate that Canada will adopt an approach similar to GDPR to give you the tools to protect

yourself. So use them.

Ultimately, it’s up to you. Be vigilant. Protect your local network. Follow good protocols. Don’t be sloppy. And be angry over every breach. Demand accountability. Next time it could be you.