BIZCOMMUNITY

Privacy vs Profit: Will 2019 be the year of consumer paranoia?

By Colin Thornton

26 Nov 2018

Our ever-present wearable device (usually a Fitbit or Apple Watch) monitors our resting heart rate and cardio fitness. We track our daily steps to get a free smoothie (and maybe even a free flight) from our health insurer at the end of the month. When paying for coffee at the local hangout, we simply tap our credit cards and rack up more points for discounts on groceries. And in Sweden, many are even ditching credit cards and opting for surgically inserted microchips.

Source: pixabay.com

Simple, seamless and profitable

Yet what many of today's 'connected' consumers are beginning to realise is that we are paying a much higher price for 'free' and convenient applications than we initially budgeted for. The trouble is, that price is only now beginning to be quantified and made more tangible to the end user.

Down the data trail

By choosing to wear Fitbits or other devices that track our health and wellness, we are creating a highly detailed, and highly valuable, data trail.

Keeping up with the connected customer
Suren Govender 19 Nov 2014

According to one analyst at Intel Security, the information that's contained on your wearable - that's stored either on your smartphone or downstream on a cloud service - is worth ten times that of a credit card on a black market. Moreover, by signing onto seemingly innocuous rewards/loyalty programmes with insurers and other third parties, we are handing that data trail over to big business.

And it's not just wearables and smartphones that leave us vulnerable. Every time we use a 'free' platform like Facebook or WhatsApp (same company by the way), we are divulging personal data with little to no idea where that data is headed (and how it's being used). This came to light with a hard knock in early 2018 when Facebook admitted that for the past several years, political consulting firm Cambridge Analytica legally obtained information on as many as 87 million Facebook users for the purpose of influencing US elections.

But let's get back to the wearables for a moment. If a Fitbit can monitor your heart rate and is sending that data back to teams of data scientists and machines to recommend the best workout programme for you, what else can it monitor?

According to experts, these devices are becoming so adept at tracking your pulse that they can accurately recognise if you are having sexual intercourse.

No surprise, then, that people are beginning to feel a little squeamish about the seemingly innocent devices that accompany them throughout their day (office, yoga, the sauna…). How closely are we really being tracked, and to what end?

Big data, big profit

The fact that so much data is being collected daily through wearable devices alone (resting heart rate, blood pressure, location, the list is endless) means that there are some very real risks attached. And with the rapid rise of the Internet of Things (IoT), whereby your fridge, TV, bedroom, irrigation system, etc, will all be connected, the risks will only heighten.

So where to from here?

For consumers, the first question to consider is 'do I need to be handing over my data to this company?' Are they using this data to help prevent a heart attack, or to influence which prescription medication I buy? Also, as a consumer, do I have the option to opt out, or at least limit the data I hand over? In the case of Facebook, which is a 'nice to have', opting out is easier. But in the case of health insurers and financial services providers, which are 'must haves', opting out seems to be an option we don't have.

Secondly, if we have ‘opted in’, who ultimately ends up with our personal data – and how will that company/individual use it? Will they sell it? If health insurers are tapped into your resting heart rate and know that you are at high risk of heart failure, will your premiums go up? And if your child’s use of online learning apps reveals some kind of learning disability, will it impact their future learning or scholarship opportunities? As we learned with the Facebook/Cambridge Analytica scandal, many businesses have no qualms about selling your data to boost their own bottom line and/or political sway.

Data Protection: Does it exist?

The next key question we should be asking is once companies have our data, how effective are they at storing and safeguarding it? What kind of measures do they have in place, and if our insurer/health provider goes bankrupt, where does our data go? As we have already seen in 2018 alone, even major financial services providers are vulnerable to cyber attacks. Liberty Holdings, for one, suffered a major breach after hackers reportedly gained access to the company’s mailing service. Where does that leave customers?

Fortunately, legislation is beginning to catch up with new technology. In South Africa, the Protection of Personal Information Act (POPIA) is likely to be fully enacted in early 2019, and is the country’s first piece of comprehensive data protection legislation.

Why privacy and security matter

Jayson O'Reilly 23 Nov 2018

In addition, South African companies doing business with European Union (EU) customers now have to comply with the General Data Protection Regulation (GDPR). Both pieces of legislation carry stiff penalties for companies that fail to comply: the GDPR penalties can be up to 4% of an organisation’s global annual turnover, while POPIA has a maximum R10 million fine or time behind bars.

Time to up the ante?

While these laws are certainly a constructive beginning to what is a highly complex challenge, it’s really up to individuals and end users to question big business and make sure that privacy and security trumps profit. Robust privacy rules and industry standards for data sharing should be instituted rapidly, because the amount of data being collected is growing at an almost unfathomable rate. Experts forecast that by 2025, there will be more data generated from sensors and devices than all of the data being generated today from every source.

In 2018, we glimpsed the perils of ‘legal’ data sharin...will 2019 be the year that consumers begin to push back?

ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SMEs is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SMEs. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...