Sorin Toma

University of NSW, Principal Adviser – Cyber Security

Managing Director

 | www.xpotentia.com | Sorin@Xpotentia.com | M: +61 419 631 023

16 April 2018

Research Briefing – *'Who is listening to your children*

A briefing on the potential access new Smart Speakers give companies to your children.

Premise

- The recent reports regarding Facebook have shed light on what many in the cyber security industry already knew. Big Tech, publicly listed companies like Facebook are accessing your personal data and providing it to third parties without your permission. As the Australian Financial Review Editorial described it, Facebook "*allowed abuse of personal privacy, democratic choice and free media – things which define a free society*".
- Many people, parents in particular, don't realise the amount of access large online companies have to private information about their lives, their family and even their children.
- With the rise of Smart Speaker devices, serious questions have arisen over how much information is being collected, recorded and shared by online companies with regard to children and what that information is being used for.
- There are also simple yet essential steps parents should take to maximise the privacy of information regarding their children in the age of Amazon's Alexa and other Smart Speaker devices.

The new age of unprecedented access to children

- Many parents will be aware that their child and likely their children's friends have Facebook pages. Some schools even use Facebook as a teaching tool. This has opened a window on the world for young minds, however it has also provided the world with unprecedented access to the private lives of families in Australia and around the world including children.
- Perhaps the most disturbing aspect of Facebook and other social online programs is that they collect and store information about the user and often use that data for commercial purposes.
- Following on from Facebook, there is a growing number of online platforms that collect, store and potentially pass on personal information. Twitter, Apple, Alphabet/Google, Amazon, YouTube, Uber, AirBNB, among many others, all collect your data. Almost always their terms and conditions protect them from liability regarding how secure our data is, instead transferring liabilities to the user.
- This new age of collecting and storing personal data, including that of children has presented a smorgasbord for hackers.

- In 2017 as many as 1 in 4 Australians were targeted by hackers. It's estimated that 86 percent of identity fraud cases in Australia were enabled using the Internet. (Equifax Report, Oct 2017 "*one in four Australians (25%) now claimed to be a victim of identity theft or fraud*")
- It's also opened the floodgates for marketers to target products and services at your kids. Unfortunately, due to the foetal nature of many new user devices, such as Smart Speakers, children are at risk of being exposed to inappropriate material and products.

Serious questions to be raised over Smart Speakers and access to information on children

- AI/Smart Speaker platforms such as Alexa, Apple HomePod and Google Home (Mini and Max) are new products and therefore still in an 'infant' state in terms of the consumer market. This can create significant vulnerabilities for users unfamiliar with the new technology. For example Amazon's Alexa supports 15,000 skills and services. This presents an extremely complex operating environment that relies on a vast number of third party systems to ensure an adequate level of cyber security. There are serious questions as to whether this is even remotely achievable, especially when it comes to children.
- With regard to devices such as Amazon's Alexa Smart Speaker, there are issues that must be addressed:
    - These devices are listening all the time – the only way to prevent this is to turn off the unit when not in use. The onus is also on the user to perform activities such as deleting historical data on a regular basis.
    - These devices do not support multiple personalities. A consumer has <u>one account</u> per Smart Speaker with multiple individuals able to use the single account. **<u>Critically, these devices do not differentiate between adults and children.</u>**
    - These devices record and store almost every piece of information spoken aloud while the machine is switched on. It will then deliver advertising based on an **<u>aggregated profile</u>** of the account associated with your home, not specific to any particular user.

      The serious issue here is the potential to advertise products and services to children without parental consent or knowledge.

      There is also the potential for inappropriate or adult oriented material being provided to children.

      This could be through the limited voice advertising ability, but also for example, **if a child asks Alexa a question, based on the aggregated profile the unit may come back to that child with 'answers' only suitable for an adult.**

      Furthermore, children may be able to order and buy products and services automatically if a credit card is attached to the account, including through voice activated purchasing.
    - The information or data gathered based on the usage profile as well as historical search record will be stored in 'the cloud' most with the potential to be located outside the jurisdiction of Australian legal system.

What can parents do to maximise personal information security?

Smart devices

- Be an informed consumer. Understand the risks. Become familiar with the setting options for your product as they will vary between products. Read the online manual – understand what you are doing and why. Search online for tips and tricks to best secure your product. There are often good online forums where you can ask questions.
- Do not connect any sensitive accounts to any AI platform.
- Turn Smart Speakers off when not in use, especially if you are having an important discussion with your spouse/partner, children and family or when you have guests that do not wish to be profiled by an AI device.
- Go to settings and change the "wake" word to something different and specific to you unlikely to be triggered by mistake by someone else.
- Setup a PIN for any purchases that will block children from being able to make unauthorised purchases. Change the PIN regularly.
- Disable voice purchasing;
- Delete your historical search data on a regular basis;

In general

- Before you purchase a particular app, smart product or platform ask yourself the following questions:
    - What is the benefit to myself or my child from this product or service?
    - What is the downside? What are the risks in buying or accessing this product or service?
    - What action can I take in case something goes wrong, such as access to inappropriate material/advertising or a personal data breach?
    - Is there a customer support line/email contact/website for lodging complaints and for resolving problems?
    - Is there a privacy commissioner, government regulator, police or any other authority that can provide assistance and or guidance?