Electronic Security in Everyday Life
Elizabeth Wilson

In the 1960's, as computers were becoming available to the public, restless citizens mused that the computers would soon have minds of their own, and would eventually take over the world. Though we now have the capability to create artificial intelligence and make robots who can think for themselves, it is becoming apparent that, in this day and age, it is the masterminds behind the computers who are starting to broaden their horizons, and acquire more control. Consider the advertisements on your phone, for example. While some of them are clearly based on your search history, people have had experiences of talking about an interest in a product, only to have it pop up as an advertisement on their computers later. Although most data is simply saved by companies to produce profiles of your consumer habits and create more effective, targeted advertising, other groups have more nefarious intentions when it comes to your personal data. With all of the different electronics that we use in our everyday lives, it is important to consider the capabilities of our devices, and the level of electronic security available to us in our everyday lives.

Alexa, a voice command technology created by Amazon, was first released to the public in November 2014 (Vigliarolo). Alongside the Amazon Echo, it was designed as a technology to be placed inside of any Amazon device which was capable of answering questions, streaming music, setting alarms, and many other features. Alexa can also tell when you're home, and saves voice recordings of whatever is said after its 'wake word' (Hildenbrand). While this device seems incredibly useful, it is also incredibly dangerous. In the best interests of Amazon, Alexa records the things you say, and by remembering the things that you ask for, along with the audio from seconds before you activate it (Hildenbrand). While Amazon uses this data to build a consumer profile for the user, these recordings are accompanied by some notable risks. Firstly, Amazon could profit off of profiles by sharing their clients' information with other companies (Vigliarolo). More likely, however, outside people who have the ability to hack your system could come into possession of your information. As the average citizen, you are likely incapable of detecting any sort of breach into your technology, so the question of a company's role in maintaining electronic security for their customers comes into question.

In Canada, rules were recently put into place regarding the notification of clients by companies if data breaches that present a "real risk of significant harm" occurred. This regulation requires that companies create assessments of the breaches when they occur and make them available to the Office of the Privacy Commissioner, including information such as number of people affected, nature of information that has been breached, and the steps being taken by the company in order to reduce the harm to their customers (McLellan). In this way, companies are held accountable for the security of their clients' information.

Companies must be diligent in maintaining high levels of electronic security for themselves and their clients. Working for a security company, I am all too aware of the things that could go wrong, and all of the information we are responsible for. When I am entering in a customer's file, I see their address, phone numbers, who they trust to be emergency contacts for their accounts, their account's safe word, credit card information, and more. When the client's contractual information is put on the computers, our company is responsible for its safe keeping,

and must take this responsibility very seriously. This information, however, isn't even the most devastating that an outside source could get possession of. Security cameras, similar to Amazon Echoes, record what they see in homes. With the ability to see and listen, it is clear why security companies need to be extra diligent in their treatment of customers' information.

While new technology provides us with new opportunities, it also creates new responsibilities for the people who are in charge of it. Conversations must be had regarding the ethics of saving information, and how this affects the electronic security of people who are using devices such as Amazon Echoes and security cameras, among other things. Despite the creation of new regulations, industries must continue to push the conversation about electronic security at the same pace their new technologies are gaining popularity.

Works Cited

Hildenbrand, Jerry. ‘Amazon Alexa: What kind of data does Amazon get from me?’. *andriodcentral.* 27 March 2018. www.androidcentral.com/amazon-alexa-what-kind-data-does-amazon-get-me. Accessed 12 March 2019.

McLellan, Melinda M., and Julie Hein. ‘Canadian Breach Notification Requirements’. *Data Privacy Monitor.* 25 April 2018. www.dataprivacymonitor.com/data-security-incident-response/canadian-breach-notification-requirements-take-effect-november-1/. Accessed 12 March 2018.

Vigliarolo, Brandon. ‘Amazon Alexa: Cheat Sheet’. *TechRepublic*. 24 September 2018. www.techrepublic.com/article/amazon-alexa-the-smart-persons-guide/. Accessed 12 March 2019.