MEMORANDUM

TO: Ms. Jackie Smith, President ABC Technology Inc.

FROM: Blake Dvarishkis

RE: Update and Implement Safety Measures Regarding IoT Devices

DATE: 12/11/2017



The purpose of this memo is to discuss and properly execute preventative measures regarding the privacy and security side of our new products. With our company investing money into IoT products, we need to ensure that our staff has the proper knowledge and tools to successfully implement safe practices regarding said products.

Much harm has been done to innocent lives through exploitation of the security and privacy of their IoT devices. In October thousands of American citizen’s DVR boxes and webcams were hacked to disrupt internet usage (Waddell 2017). The cable company, the affected customer, the manufacturer, and everyone down to the programmer would be at fault for an incident like this, hence why our company should lead the trail and set an example when designing IoT products.

Kaveh Waddell talks discusses the many ethical concerns regarding the distribution and potential usage of IoT devices in his article “The Internet of Things Needs a Code of Ethics”. Technology betters itself faster than what societies can keep up with regarding legislation. This creates an abnormal responsibility load on product designers and developers to decide what is and is not ethical when handling people’s privacy. His solution is a simple one, really consider when designing a product what its intended use will be and how its security for said uses could be affected. Instead of letting problems come first then reacting with concerns, consider the concerns first then design a product around the mentioned concerns. The company’s stake, employee’s lives, and customer’s lives could all be affected in the long run in the absence of these protective measures.

If our company were to lead the initiative on producing and using these IoT devices, many potential lawsuits could ensue. When handling citizen’s personal data, we need to be transparent with what we are recording and have the outmost safety of others in mind when managing their data. Our reputation would plummet if we were to have a publicized failure with any sort of incident involving an IoT device. Security must be a main priority when manufacturing IoT devices. This is why our production managers should henceforth step back and observe the failures from other companies with their products and to always follow previous guidelines with respect to security and privacy.

One must be vigilant when working in gray areas such as this. If our company does not learn from the mistakes of others then we could potentially lose money from lawsuits, our products would no longer be in a high demand, and as our reputation decreases, many of our stockholders will want to get rid of their shares, leaving Acme Technology with empty pockets and a tarnished name.

The world of IoT devices is an ever-expanding one with many interesting new frontiers. It is in our best interest to keep up with the law, always be safe, and to learn from the mistakes of other companies when navigating in these treacherous waters of security and privacy. In the event of any questions or concerns please contact me at [blake.dvarishkis1015@gmail.com](mailto:blake.dvarishkis1015@gmail.com) or 402-309-0878.