TENSIONS BETWEEN PRIVACY AND SECURITY

The tension between personal privacy and security deals primarily with the amount of data that is circulating around the internet, or the “Cyber Reality”, simple services require one to give away too much of their personal information that is then stored on that organizations data servers. Now, there are laws in place to protect our information, but these laws have loopholes that allow branching or “family organizations” to mine, view, and use consumer data so that they may better the service for their consumers. The concern over how m uch information an organization has on its employees or how much information (if any) the government has on its citizens is only coupled with the concern of how that information is used by a corporation or government. To address this tension, we have to think that there are two sides to this particular tension. The two sides are: people who believe that the American government is not doing enough to secure them and their information while the other side believes that the government is doing too much to protect them and their information. The side that believes that the government is not doing enough may be thinking that information should be protected by the laws and regulations that are in place today, but updates and revisions are needed to the laws that protect that information. Coupled with firm security measures in respects to handling sensitive information such as PHI (medical), PII, NPI’s, banking and other information that can be deemed sensitive. In addition to having parent companies collect, compile, and store information “child branch organization” that are linked to the parent organization also have certain access to the data that is linked to the main corporate branch. The other side believes that the government is doing too much to protect them and their data in respects to current data practices and laws. They believe that the government and any or related organization is collecting too much information and or setting restrictions that restrict an average person’s civil liberty rights. This side also believes that these massive organizations are using their data in a way that can sell them or in retrospect harm them by collecting and redistributing their sensitive information to third parties and other affiliates. This will be discussed in the preceding article.

We have laws in the U.S that govern how personal information is used, stored, collected and distributed. An organization or corporation cannot redistribute data, the corporation cannot disclose any sensitive information,

sensitive meaning information that includes your bank account data, SSN, your recent or ongoing medical data (such as treatments, recent surgeries, vaccinations, etc), or any information that is deemed sensitive without having your written permission first. These laws are not perfect however as they have their own loopholes. HIPAA, or Health Insurance Portability and Accountability Act, is one of those laws, although complex in a sense that there are many parts and sections, that not only protect a person's health data privacy but also a person's data/personal security. It was instated to (help) protect your Personal Health Information (PHI) – But a healthcare provider or a branch entity of that medical organization has some form of permission to view or use that PHI if it is related to treatment, medical payments, and other healthcare operations. COPPA is another law that has been expanded upon in regard to information collected from minors online hence the acronym Children's Online Privacy Protection Act which regulated personal information collection of minors on the internet – This law has an exception; however, this exception will allow the collection of data if the operator of the data storage unit is capable of keeping that data secure and or confidential. There is also the Gramm-Leach-Bliley Act (GLBA) that is a massive banking and financial law that has important data privacy and security requirements "built into" it's documented roots – But there is a loophole within this law and this loophole entails that branching "child companies" or organizations have [some] access to that information in order to process transactions, make recommendations, and allow certain account actions to be executed.

As discussed above, the U.S has laws that "limit" what organizations can and cannot do with your personal information but, these laws are not perfect even when they seem like they are. This is where the tensions become a little clearer in regard to personal privacy and data security. You have these laws that are instated to protect you and your PI (Personal Information), this information, when breached, can have life-long or equally damaging effects. Third parties are an exception however because they are tied to that specific "parent" organization. These third-party affiliates choose what they want (and don't want) you to know about them and their practices (in proprietary sense) which brings up the question: what will happen if that third-party affiliate is breached. It cannot be stressed enough that these affiliates are tied to a certain "corporate family" and have access to that organizations data. If that affiliated branch is hacked or certain section(s) of that affiliates network (which mines and stores the data) is breached then the results can be devastating, so devastating in fact that it can have a lifelong impact on the persons and organizations affected by that breach. A few of these breaches (OPM Hack, Operation Aurora, Target, eBay, Anthem, and numerous other

major organizations) have lasting and often times lasting, damaging, effects on the customers that were serviced by these organizations. The Anthem data breach (an example of a medical data breach), where millions of customers names, birth dates, SSN, street addresses, e-mail and employment information and even income data was stolen in a massive healthcare break-in. The OPM breach is another example. The Target data breach in which 40,000,000 units of credit card information was compromised. This breach occurred because "The computer was installed by the HVAC company, and the company left all passwords at their default values." (Examination of Challenges, pg: 7, 1)

With these massive data breaches comes growing anxieties over how data is managed by organizations and their branching affiliates, people become more and more anxious when they research or sign up for certain services like credit card services or medical services but the big issue relating to anxiety is the amount of data organizations store on their consumers. This brings us right back to the statement that the tensions of personal private information and information security, although divided in terms of statistics, is not one sided at all. The tension comes from the fact that massive amounts of information is being collected about people for services. For many, to use a service such as banking, medical assistance, and even car buying requires the relay of personal information from one affiliate to another whether it by phone or by electronic transfer and that those bits of information although being "bits" are still large and can affect a person's chances of receiving certain services or buying or acquiring certain "goodies" and some of those bits of information is unknown even to the holder or user that uses a certain service as a base point for information transfer (a banking firm). The Credit Score System is one of those unknown services. How is it calculated? What sorts of information is accessed in order to determine a user's score? Why does it affect what I can and cannot do? Well, we know that Big Data is involved when dealing with credit score. We also know that, from the reading The Scored Society that Big Data is mined to "rank and rate individuals" (Scored Society, 2). The keyword is Big Data the system uses predictive algorithms to predict the actions or future actions that people may take in future purchases and or transactions along with what, when, and where that transaction took place. The system then places us in categories such as "good credit risks, desirable employees, reliable tenants, valuable customers—or deadbeats, shirkers, menaces, and "wastes of time." (Scored Society, 3). People are often worried about their credit score in a sense of what is being analyzed during the calculation process which brings us back to the parent and sibling corporations and what kind of data they have access to. This only adds to the anxieties people have about not only their personal

privacy but also the security of their data and what happens or what an organization does with that data.

In conclusion, many aspects and laws play a role in the tension between personal privacy and security. To reiterate, you have laws in place that prevent big corps from doing whatever with your data (redistribution with permission, selling sensitive data, having complete control over your data, etc) but, alongside that, these corporations have subset corporations (or third parties) that have access a portion of that data, what data portion they have access to is unknown to us consumers except what is written in the TOS for consumer data of that organization. To put it simply: the tension is how much data is being collected, how does it affect the personal privacy of the average consumer, how is the collective data on an average person used to defend us against domestic and foreign threats, and most importantly: what is being done with the massive amount of data that is collected by not only the government but also corporations. Another tensive aspect would be the utilization of this massive collection of personal, private information to help/ assist consumers in protecting them or assisting them in making “better choices” in their lives. That is the tension in balancing personal privacy (with laws and regulations) and security.