Fixing the Issues of a Video Broadcasting Site

In my midterm paper, I wrote about creating a video broadcast website similar to that of Twitch.tv. Within this, I talked about the many issues that could arise with the creation of such a site. Of these there were two that were very similar being what types of data would be collected and measured by the site and do users have the ability to access such information. So how do we handle these issues and ensure that both consumers are informed of what data is collected and how they can access such data. To do this we can develop policy within the company to teach and follow the Fair Information Principles, which was covered in our course book, within our development of the application. This means among many more ideas that the company is dedicated to ensuring that we only collected what is needed, keep that data for only as long as needed, provide users the ability to correct and access information collected on them, and secure data from actions like theft and leakage.

To make this policy a reality and not just the idea of following the Fair Information Principles, we need to develop an in-depth software development life cycle for the broadingcasting website. As we talked about in class, an SDLC helps define testing and training needed in the development of software. So with our website, we will need to ensure that workers are taught the privacy ideas within the Fair Information Principles. As well, developments need to be tested to ensure that a user has the ability to know what data is collected before signing up for the service and have the ability to retrieve the data and correct inaccuracies in the data.

But how are we going to prevent acts like theft or an insider leaking to protect the data we have collected? One thing we can do is follow the idea of least privilege to prevent unneeded access to data, so only qualified people can be allowed access to more sensitive data. To do this, we would likely use items like RFID cards that are used to unlock rooms to identify people with the proper authority. As well, workers could need software to generate one-time passwords as a form of multifactor authentication. These systems like this help reduce the ability of people to steal a workers device or just walking into a corporate building and being able to gain illegal access to company systems.

On top of the Fair Information Principles, the company's policy should consider the ideas of informed consent and the de facto standard of the California Consumer Privacy Act (CCPA) that was talked about in a reading from Vox.com. This ethical idea and California law are good standards that coincide with the Fair Information Principles. These, respectively, are a way to ethically ensure that the users are able to accurately understand and agree to the use of data collected on them and a law that provides rights to access certain information collected on users. These help minimize the threat of the risks I identified earlier along with the Fair Information Principles and should be taken into consideration when developing policies and software.

So with a policy that focuses heavily on the privacy and consent of the users and following many different ideas and laws to shape aspects of said policy, there are bound to be some rejections of ideas. One such idea is to minimize what data is collected and how long it is stored on users. Some people might bring that more data and different data being collected on individuals can be used to make more money through specific sales or personalized ad systems. As well, removing the data after sometime means that we are in a way throwing away potential sales. Another idea could be rejecting why the policy has such a high focus on training peoples and testing systems or the web application. Doing these things can be seen as wasting development time and as we all know time is in fact money. These ideas are vital to the policy I would want to develop that protects users but on a business side of things is less than ideal and means a loss of profits.

To those that reject the idea of minimizing data collection, I would argue that collecting more data creates a potential greater impact to the company if a breach were to occur. The idea of impacts that we went over in class to a business perspective is basically what is the actual loss, like monetarily. So when there is more data to be collected we further complexify our systems and create more info that could be potential stolen. When that occurs, we would incur more monetary damages to the company, so to compromise I would say that we could try to find a balance to min max data collected and income. Now, as well, there are those that don’t agree with the idea to remove data after a certain amount of time since we could still use it to earn revenue. To them, I would argue that after a certain point of time the data collected someone loses it value to help predict what they would want to watch or be useful to advertisers. So keeping adds to potential impact to the company and users data as there is more being stored but not being useful. This has the same problems as the idea before with impact creating greater monetary harm, and we should set out to find at what point would be best to remove unneeded data on users.