The security of personal information

Science, Social Science

The paper " The Security of Personal Information " is a wonderful example of an assignment on social science. Every person has different views pertaining to privacy, particularly when it involves personal information. The problem today is that personal information is given for financial, recording, and other important purposes that may be accessed public because of the World Wide Web. The problem really is that we ourselves give out information about ourselves, and some laws require us to give it away to certain agencies even though we don’t want to. It is a fact that privacy must be protected, but there should also be a limit to how “ secretive” a person could be. There are times when it is for a person’s best interest that information about him/her should be made known. Data protection is an important issue. Companies or agencies must declare what data they are using as well as for which purpose they are using the information. Additionally, only relevant information should be stored, those that are needed should be discarded in order to protect the person concerned. On one hand, today’s advanced marketing systems want to use personal records in order to target specific services for certain individuals. This availability of records has made background checks easier. The great thing however is that the government of Australia is taking steps in order to protect its citizen’s privacy. The government has formulated laws restricting the kind of information any agency might require. Examining mails and tapping phone lines are also deemed illegal unless mandated law. As individuals, we have certain responsibilities to help protect ourselves. We should know and monitor the information we give away and the purposes of its use, after all our safety lies in the security of our personal information. The Issue of CensorshipCensorship is a hotbed for debates among the

general public. Certain countries set limits when it comes to access to certain sites and information. For example in the US, the government is seeking to limit or at least monitor the propagation or access of pornography on the Internet. The same goes for Germany who absolutely prohibits the right to use Neo-Nazi sites. In China, the government has agreements with ISP providers. All of these countries have there owned ethical reasons for the prohibitions. There are many kinds of censorship. There is one imposed by a governing body and the other a kind of self-imposed censorship for personal reasons. The censorship that is imposed by a governing body is usually done when a certain material does not coincide with that governing body's belief or standing. The other kind of censorship is when a certain author, publication, or etc decides to censor their material for fear of recrimination from the government. It may also be that they are simply monitoring to which audience the movie, music, information, would reach. The difficulty with censorship on the internet is that there is no way of knowing who is accessing the data. What's more, the internet is too global and massive for the censoring body to control. According to Immanuel Kant, there shouldn't be censorship because human beings should be able to control themselves or use their rationality and know right from wrong. Man has dignity and it is that dignity that will lad them to make the right decision, so there is no need to censor anything at all. On the other hand for Mill, every information in itself is valid. Censorship is regulated in Australia. They do not just censor everything there are guidelines and qualifications when censoring the data on the internet, film, or any kind of media. For the Australian classification act information, film, music, etc should be identified as to its merits,

morality, relevance, and even the people who made it.

CybercrimeTechnology which was built in order to make our lives easier seems to be have made it a little bit inconvenient and for some people downright difficult. Computers are used to sabotage, steal identities, steal money, and a whole lot more. Cybercrimes are costing governments, companies, agencies, and people their lives, finances, and reputation. It has been estimated that billions are lost all over the world because of crime committed over the computer with the use of the internet. The most common target is financial institutions. With the advent of the use of computers criminal opportunities have also upped the ante. Crimes are not just committed via the internet; fraud and counterfeiting have also increased because of the advancement of technology. Unfortunately, financial institutions are not making any move because there are scared that they will lose consumer confidence. Information theft is the most common motive for cybercrimes. Even reputable companies resort to stealing information about rival corporations to gain advantages. The Federal agencies in the US are often condemned for their lack of computer security. Unfortunately, they admit that computer safety is not exactly a top priority when it comes to the government budget. Hacking is a widespread problem, but at times there are certain types of hacking that could actually help, like if the company wants to test its security measures. Technology is now participating in politics. Online voting has been proposed in the US in order to make counting and organizing votes quicker, but cybercrime incidents are making people cast their doubts. Today there are certain agencies that are taking steps by creating task forces against hacking. There is also the proposition of

disposable credit cards: one card per purchase. For added safety, there is cyber insurance that takes care of damages for a certain compensatory amount. Technology is now participating in politics. Online voting has been proposed in the US in order to make counting and organizing votes quicker.