Surveillance and privacy research paper example

Law, Security

The issue of privacy of persons has become a common point of argument in many countries. Several people incessantly complain that social network sites have scrapped all the privacy of individuals. However, the latest area of concern is privacy of internet users. Currently, due to the rising cases of insecurity and threats of terrorism, most governments have initiated modalities through which peoples information can be shared through various organizations inclusive of governmental security offices. To top it off, video camera surveillance systems have been fitted in residential houses of individuals, workplaces, and all other public places such as social places. Many have argued that the installation of these surveillance cameras in almost all places have scrapped the privacy of individuals away, which is a basic need for all citizens of America. This has necessitated the government to come up with various solutions towards the privacy of American citizens. This essay endeavors to probe some of the suggestions and recommendations, which could help solve the problem of privacy of Citizens in America (Davies 105). Veritably, there is a paucity of information that touches on the onset of the usage of video camera surveillance in the U. S. thereby making it difficult for one to accurately pinpoint when this started being a widespread issue. Nonetheless, it is noteworthy that in 1986, Congress passed the Electronic Communications Privacy Act which countenanced law enforcement agencies to use the flourishing technologies such as video surveillance to help curb the problem of insecurity. The New York Trade Center bombing presents one of the recent examples applying the 1986 Act. In this example, a primal confidant of the defendant witnessed against the defendant. Resultantly, the FBI was able to conduct an all-

encompassing video surveillance, between April and June of 1993, of the defendant at his home, amassing the evidence that was used to declare him guilty. Although video surveillance can be utilized for unethical purposes, it also has many legal and beneficial purposes for its use. Some of the more common debated issues about video surveillance are for video surveillance on the roads, video surveillance usage in unethical ways, and the use of video surveillance at the workplace.

Closely related to the Electronic Communications Privacy Act and on which this paper is primarily based on is The Cyber Intelligence Sharing and Protection Act (CISPA). CISPA is a bill designed to let companies freely share any and all information of their online users with other companies and the United States federal government, as a whole, in the name of “ Cyber Security.” Though not state what part of the government would get the information, the bill states that if a potential cyber threat is detected, the information on that person is encouraged to be forwarded to not only the Government yet any other websites or companies that may be affected by said threat and any organization that does so will be exempted from any possible legal issues.

All these are done in the name of “ Cyber Security”; a phrase that is not given any succinct definitive description in the act. Nonetheless, the broad language of the bill makes any and all privacy online within the United States and only within the United States, completely a thing of the past. It is worded so that the bill literally overlooks any and all laws currently in place, including every single amendment to the constitution and the constitution itself. This bill is virtually a power in and of itself as opposed to a law within a

government- an attribute that rendered this bill a monstrosity of a problem. Recalling vividly, this all started around the year 2010 when the film makers of Hollywood and many other special interest groups decided that they wanted stricter laws on fighting piracy. While the Digital Millennium Copyright Act is widely believed to be entirely sufficient when dealing with the guys who said that the VCR and the MP3 player were tools of piracy and would completely destroy sales and the entertainment industry. Avoiding the fact that the entertainment industry is stronger than ever their constant use of the term “ piracy” as well as other scare tactics have people thinking that piracy is running rampant everywhere , and they’re losing billions of dollars, apparently, such beliefs are further from the truth than said special interest groups would ever want anyone to realize, the fact is that they simply want complete and total monetary control over all artistic media and are pressuring the United States Government with millions of special interest dollars to design yet another antipiracy law as the Digital Millennium Copyright Act that they had installed simply is not enough for them. Everyone in the United States or anyone that does any business with businesses within the United States that have personal information stored on the internet in some way, via company data files or the like is at risk of having their information distributed to everyone and anyone in the name of “ Cyber Security,” as vague a term as it is. This means that potentially billions of people are at a major personal risk of having their information go public, after all the transfer of files such as that can be intercepted or misdelivered, thus with the transference of said information becoming not only more likely yet actually encouraged then the accidental delivery or the interception of

that information will become easier and equally more probable. Additionally, with call of “ cyber security” multiple companies can obtain users’ information and then say they’re securing the web by offering users ads that are already tailored to you or some such thing. While that may sound unrealistic, it is all the justification that this bill would require and the companies that gave and received the information would be entirely safe from legal harm.

As stated earlier, such developments have led to the infringement of people’s privacy. Even as this developments are crucial with regards to the provision of dependable security solutions for all, it is high time some amelioratory suggestions are given in a bid to safeguard the privacy of individuals while also providing a reliable security to people. One of the most radical and likely unrealistic solutions to this problem would be to invoke a nationwide, or even international uprising, and then proceed to lynch, tar and feather, and do other angry-mob-like things to rid of the politicians as well as those undesirables whom are in favor of this legislation and any like it. This particular solution would not only remove the threat this legislation poses to everyone world wide it would also remove any future threat from the greedy special interest groups that attempt to have the legislation made into law. Furthermore, this would be the most idyllic situation simply because it would get many people involved and show the governments of the world that they should serve and fear the people, not the other way around.

However, this would also be the most drastic method. It is not a utile method for any little thing and getting even ten people to care about something, let alone millions or billions, would take a great deal of effort. This particular

solution has the potency of engendering more troubles than it solves, yet with such a chaotic and unpredictable solution to such a predictable problem it is uncertain what more it would or could accomplish. Overall this particular solution is not only radical it is outright extremist, however, it is always good to think up some unlikely solutions first and then get to more rational ones later down the line.

A second, less radical, solution would be to start a major campaign and raise even more funds than the special interest groups in Hollywood and other such locations and use that to push the agenda of freedom of speech and right of privacy even on the internet. This is a favorite tactic of big businesses and the obscenely wealthy, throw enough money at it , and the problem will fix itself. The only things that tend to hamper such a tactic are the masses of people that go against all that money, and in fear of their lives and jobs the politicians then, usually, concur with the people and not the special interest groups with a lot of money.

However, the special interest groups tend to fire back by waving more money around and eventually the politicians, feeling the pressure of money and job threatening civilians up in arms, often make a compromise, which can usually sound better than the original yet is often just worse, or the same as the original piece of legislation being pushed through. So in such it only makes sense that a solution to the problem of CISPA would be to not only mass as a people, yet also get a bunch of money put together and throw it at the politicians as well, thus “ encouraging” them to listen to the people in lieu of the special interest groups.

Yet another, and likely the most rational and efficient solution for the problem created by CISPA is to simply protest. Announce our position, petition, get people involved, tell the people the facts; people should be made aware that their personal information can be transferred under this bill and that they will have no rights on the internet in a bid to beef up Cyber security. It is obvious the special interest groups will not stop until more legislation on cyber security is passed, so support something that makes sense. For instance, there has been talk of other legislation that deals with cyber security that allows a similar thing to CISPA, only it would secure crucial and key locations, such as water facilities, food processing facilities, actually crucial and important infrastructure that is key to living in this day and age. From a personal point of view, this solutions is perhaps the most realistic and certainly one of the fantabulous solutions to the problem of the privacy problem emanating from the enactment of CISPA. A whole new piece of legislation that secures crucial infrastructure and leaves the privacy of the private citizen absolutely private in the process is undoubtedly the key to the whole cyber security debacle. The companies should not expect the government to safeguard their own assets as the government is here to serve the people, not the corporations. In the past it has been evidenced that any business venture had to deal with outside threats mostly on its own, it had to secure its own assets and demand retribution for any stolen or harmed assets of its own accord and, in general, it worked out fairly well.

As for criteria for my favorite solution, it is simple. The final presented a solution to CISPA would no doubt secure crucial parts of the online infrastructure of the United States of America, it would not violate the rights

of the citizenry nor would it have the power to supersede any laws set before or after it. It is these things that are needed to secure the citizenry of the U. S. both privately and publically. In such this writer feels that the final presented solution here is preferable to others because it secures the truly important things against cyber attack, it does not give the legislation excess power or limited power, and it keeps the private life of the private citizen utterly private, which is the whole point of calling a private citizen “ private” in the first place; in a manner that this solution addresses the whole issue of privacy presented by CISPA.

Work cited

Davies, Simon. Big Brother: Britain’s Web of Surveillance and the New Technological. London:

Pan, 1996. Print.