Trevor Karl

C00441253

CMPS 310-001

Lecture 4 Questions

1. Event organizers who are viewed as potential terrorists absolutely should not be able to use video surveillance systems to identify potential targets. If anything, the “event organizers” are obviously trying to cover their tracks as possible terrorists in order to blend into the public without raising any suspicion all the while advancing their plans. For the argument that the potential terrorist event organizers should be able to use surveillance systems for targeting, it would be an ingenious idea that allows them to fly under the radar of law enforcement services. Plus, the “event organizers” could argue that they have the right to use the surveillance system to ensure the safety of the eventgoers. However, law enforcement services have probable cause to shut down the event that is occurring in order to keep the general population safe, and possibly arrest and interrogate the supposed terrorists. In conclusion, the suspicious event organizers should not be able to use the surveillance system due to the possible endangerment of a population larger than those attending the event (protection for the greater good).
2. An opt-in policy is when the collector of information may not use it for secondary use(s) unless the person checks or clicks a box (usually) or signs a form permitting the use of his/her information. An opt-out policy is when a person must request (usually by a check box) that an organization does not use his/her information for another use. Essentially, an opt-in policy is a less sketchy approach when collecting user information since the organization will be straightforward with asking the user for his/her information while easily allowing them to choose not to give away his/her information for any other use. The opt-out policy pretty much takes user information and uses it for secondary purposes without really asking outright, and most of the time a user would have to go into privacy settings of some software (such as Nvidia or Steam) and opt-out of receiving third-party emails, newsletters, etc. Plus, an opt-out policy automatically assumes a user will be fine with giving out his/her information for secondary and will have boxes checked already on a site instead of leaving them blank like an opt-in policy. So, if a user is on a site with an opt-out policy, he/she needs to be extra careful when reading a site’s agreements since the user could accidentally allow his/her information to be used for other purposes by making a simple miss click.
3. Although criminals can steal a person’s information and his/her expensive car, it is far more serious to have personal information stolen than it is to have an expensive stolen. Because criminals now have a person’s personal information, they can do far more worse things than just stealing a car. The criminals can pretty much take a person’s money from his/her bank account, overcharge credit cards, impersonate a person online or over the phone with eerie accuracy, which boils down to pretty much ruining a person’s entire life just by stealing all of their information from the database it was stored on. When it comes to stealing an expensive car, the only thing the criminal is going to do with it is drive it around or sell it for more money, making it nowhere near as useful as having a person’s personal info. Plus, it is there is a chance that the person who got his/her car stolen can get a relatively quick insurance payment from the loss, while identity theft can take years (if not more) to fully recover from. The analogy between a stolen expensive car and stolen personal information is somewhat similar, and the best insight drawn from the analogy is that a person needs to ensure that his/her physical and nonphysical valuables are as safe as they can possibly be no matter what.
4. When it comes to social media and others posting images of another person with or without his/her permission, the reputation of a person can be forever tarnished and engrained in the minds of individuals who see the image/video spread like wildfire across the entire internet. Plus, with the fact that videos and images tend to stay on the internet forever -- whether it is on some database or some random video streaming site – people must absolutely be careful when it comes to posting stuff about others online, and people who choose to do so should almost always ask permission from the other person in regards to his/her right to privacy. Obviously, circumstances in which a video/picture of a person are seemingly embarrassing, offensive, or reputation harming in anyway should have permission from the other person before being posted since it can technically ruin his/her entire life (as in possibly losing a job, having a hard time getting a job due to being a well-known meme, etc.). However, it can be a courtesy to post something about an individual without his/her permission if the post praises the person or increases the person’s reputation in a non-infamous way. When it comes to feeling ethically obligated to post something about another person without permission, it would have to expose the person for heinous crimes and malicious doings. For instance, there are constantly videos and images being posted on the internet about politicians/government officials and their constant corrupt actions, such as with the relatively recent Jeffrey Epstein incident. There have been consistent leaks about how Epstein is pretty much a prolific pedophile and how it relates to the conspiracy of how he was killed in his prison cell, and ethically speaking, this helps to uproot and expose corruption of powerful people that the general populous relies on for leadership and guidance.
5. Privacy for every individual is a negative right itself since every single person naturally deserves the option to keep to themselves. Although not explicitly stated in the 4th Amendment of the Bill of Rights (which is filled completely with basic liberties or negative rights), “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…” implies that individuals have a natural right to privacy. However, privacy can also be a positive right that relies on others to provide that feeling of privacy for an individual. With access to the Internet nowadays, websites typically have cookies that can keep track of what a person looks at and his/her information, which prompts websites to add opt-in/opt-out features when it comes to using user information for other purposes (essentially, individuals are relying on organizations to keep information private). The most appropriate right to consider privacy is definitely as a negative right since every individual deserves some amount of privacy without having to rely on another party to ensure the privacy. Plus if a person has to rely on others to ensure his/her privacy, does that person necessarily have privacy when others clearly have knowledge about what he/she wants to keep private?