COMP 4730, Section 002  
Fall 2019

Final Paper Assignment

10 case studies of your peers have been selected and gathered and compiled in the document below. For the paper portion of your final assignment (10 points for the paper and 10 points of the oral presentation) please read through each of these 10, and fill out the below table for EACH.   
  
Submissions are due Tuesday, December 3, 11:59 PM in Canvas. Late submissions will not be accepted on this assignment.

Any table that does not have the Case Study Title listed will not receive any credit for that particular case study (equal to 1 point).

**COMP 4730 FALL 2019 FINAL PAPER**

Study the 10 case studies posted on Canvas, review the ACM Code of Ethics and Professional Conduct at <https://www.acm.org/code-of-ethics>, analyze each case study from the standpoint of topics discussed in this course and in the textbook as well as the ACM Code, then fill the table below for each case study, and submit the ten tables as a single Word or PDF document by the NEW DEADLINE OF **11:59 pm Tuesday December 3**. NO LATE SUBMISSIONS ALLOWED. Grading: 0.2 point per question except for the case study title (which MUST be provided).

|  |  |
| --- | --- |
| Title of the Case Study |  |
| What is the most important ethical issue in this case? |  |
| What is ONE ACM Code of Ethics and Professional Conduct principle (state the principle not just its number) that applies to this case and the ethical issue you identified? |  |
| State one PRO argument concerning the issue |  |
| State one CON argument concerning the issue |  |
| What is your decision or which side (pro or con) would you choose AND why? |  |

**Case Study 1**

On September 17, 2019, just a few weeks prior to the writing of this paper, the District Court of Paris made a radical new ruling regarding the ownership of software. In the case, referred to as UFC-Que Choisir v Valve, UFC-Que Choisir, a French consumer rights group (“Que Choisir” roughly translating to “what to choose”) alleged that Valve, the privately-owned creator and owner of Steam (by far the world’s largest platform for the sale of digital video games), was restricting users in a way contrary to EU law.

On Steam, as with most if not all similar platforms, users do not have the right to resell any games they purchase. Once a game is played by a user, the game cannot be traded or sold to any other account. This is contrary to physical copies of video games which, as per EU law, are considered goods and may therefore be traded or sold freely as long as they were obtained legally. The situation is similar in the US – legally obtained physical copies of video games can be sold or traded at will. The important question, at least as far as it concerns users in the EU, is if digital copies of video games are also considered goods.

In the past, digital copies of video games have not been considered goods. An identical case was brought in 2014 to the Regional Court of Berlin, where the court dismissed the case and permitted Valve to continue restricting the resale of its games. Valve’s primary defense for this issue was the claim that Steam is subscription-based, and therefore anything on Steam was part of this subscription rather than an independent good. UFC-Que Choisir fired back at this argument, stating that since users do not pay any fee to use Steam, and since they pay the full cost of games up front with the expectation that they will be able to play that game indefinitely as they see fit, Steam is not at all a subscription-based platform and should be treated the same as any other distributor of goods.

Ultimately the District Court of Paris decided that Valve’s subscription defense was not a compelling argument, and ruled in favor of UFC-Que Choisir. The court decided that Valve must allow all French users to resell or trade their purchased games on Steam, and must notify French users of this change. The change, however, would likely be much larger than just France. Since France is part of the EU, this ruling would undoubtedly affect the entire union – this is not a law specific to France, so it sets an extremely strong precedent for any similar cases elsewhere in the Union. It would also likely affect the rest of the world as well – consumer groups in the US would certainly try to follow suit, and there are numerous platforms similar to Steam owned by many different companies that would almost certainly be held to similar standards.

According to journalists at Kotaku, a Valve representative has stated that the company has submitted the case for appeal and intends to make no changes to their current policy during the appeal process. Regardless, this case is a landmark ruling to consider with regards to the ownership of digital media.

**Case Study 2**

Case Study Description: FBI vs. Apple

On December 2, 2015 in San Bernardino, CA, Syed Rizwan and Tashfeen Malik attacked a government training event and Christmas party for the San Bernardino County Department of Public Health. In their attack they opened fired on attendees of the event using several different firearms. Their attack resulted in the death of 14 people and an additional 22 people were severely injured. In the aftermath of the attack a very important debate over computer encryption technology took place.

After the shooters were killed in a shootout with police one work issued phone belonging to the shooter was seized by law enforcement officials. Although they seized the phone, which was an Apple iPhone, the phone was set to eliminate all data if ten incorrect password attempts were made. Due to this, the FBI sent orders to Apple to create new software which could bypass the password protection and give the FBI access to the data on the phone. The goal of the FBI was to extract data which could aid them such as contacts, photos, messages, or calls. In order to get Apple to help with this, the FBI was able to obtain a government order from a circuit court under the All Writs Act of 1789 which would force Apple to assist them. In response to this request Apple CEO Tim Cook made a public announcement that included the following words:

“Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone…If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone’s device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software…Opposing this order is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.”[1]

After Apple ignored the order and declined to make the software, a hearing was scheduled where Apple representatives must appear; however, just prior to the hearing the FBI was able to access the data by using an unnamed third party which resulted in the freeing of Apple from the orders. Although the legal battle never took place, this chain of events again raised the question of how far the government can go when it comes to citizens privacy, and how far they can go in forcing companies to access data on their products which are sold to citizens.

**Case Study 3**

Case Study:Theft of U.S. Intellectual Property by Foreign Entities

In 2013, a Huawei engineer was indicted for the attempted theft of a robot arm designed by T-Mobile. This technology, named Tappy, would mimic the actual taps by a smartphone user in testing the features of a phone as if a real person were operating it. If this robot had not been recovered, then the value of Tappy would have been more in line with the norm and contributed to the aggregate loss of US intellectual property to foreign entities. In fact, each year in the United States, the private sector loses between 225 and 600 billion dollars due to stolen intellectual property by foreign governments, particularly China. The intellectual property that is obtained without the permission of an estimated 20 percent of American companies can range from patents to trademarks and from copyrights to trade secrets. To put that into perspective, the US current dollar GDP increase of 4.6 percent in the fourth quarter of 2018 alone could have nearly doubled if the theft of this IP (Intellectual Property) were either prevented or if the Chinese and other foreign entities were to rectify this dollar for dollar.

One of the relevant ethical issues is how to protect United States intellectual property without risking an escalation in the trade war. Another relevant question is how to enforce possible compensation for damages against the United States, especially if it is unclear whether these foreign entities were affiliated with a foreign government or completely independent of the government’s control. It is certainly in the interest of the United States to “provide for the Common Defense” and protect the property of its citizens, and by extension the property of the citizens that make up an American company. However, the US government must also consider the possibility of warfare, and the potential economic loss of increased tension between US companies and foreign entities abroad. If the projection for these losses due to proactive response were to outweigh the existing, recurring losses, then the US may resort to a more passive strategy of mitigation. For instance, the US could continue gathering data to publish the estimated value of the theft. This may indirectly encourage US companies to adopt more effective information and cyber security practices since they believe it to be a real threat. Another passive strategy that the US could employ would be to either subsidize information security or regulate the private sector and to enforce this business law with a government organization, perhaps behaving much like the Federal Trade Commission. Such minimization strategies are not necessarily my proposed solutions to the broader problem, but scenarios for imagining what an almost completely defensive strategy by the US would look like.

However, in recent events, the United States has responded by going on offense, applying pressure when in trade negotiations with China in particular, since either the country or its constituents have been the primary culprits of IP theft to date. In fact, the Trump administration leveraged a 50-billion-dollar tariff on Chinese goods to counteract the monetary losses of American companies. The Chinese government responded. In 2017, President Xi Jinping called for harsher punishments of those who commit these crimes, but the Chinese have lacked an “effective enforcement strategy” and have had “insufficient means of punishment for offenders.”

Considering all these events and interests, this forms the ethical problem on which I will base my case study. My analysis will focus on the theft of technology, computers, and software since this subset of intellectual property is more germane.

**Case Study 4**

**Case Study on Tracking Chips**

Kidnapping in the United States happens often and leads to unsolved missing cases, solved children deaths, and stressed disrupted families. So, the government decided to find solutions to narrow the chances of children going missing and never being found. The government concluded that children should be implanted with microchips at birth, and microchips will also be available at cost, for anyone else who chooses to have one. This invention will give each person a personal identification in which they will be tracked by. There will be a remote device that is used to locate the microchip and the device can be connected to an app as well. The guardian/s of the children can have access to the remote tracker app, and anyone else who is granted access by guardian.

In addition to the tracking, the government wanted to make microchips from positive motivations, not just from negative. Which lead to the ability to use microchips in collaboration with new technology innovations. It can be used as paying forms by connecting the ID to your bank account. Also, the government is allowing hospitals to allow the microchips to be used to check in with and view health information. The microchips will be able to check and update your vitals as well. The remote device will allow you to view your vitals and alert you of any health concerns.

**Case Study 5**

Case Study Description - The Right to be Forgotten

The “right to be forgotten” is the belief that people should have the ability to control what information about them is published or kept private. This information includes videos, pictures, information, and all other data that have been collected, published, or released to the internet and other sources of media. The thought process behind it is that a person should have the ability, after a period of time, to rescind information that impedes on the privacy of the individual and is potentially harmful for the individual’s future endeavors. This idea is largely considered to be a natural human right in many countries in the western world including the entire European Union and the United Kingdom, and there are forms of it in many other countries as well.

This right to be forgotten is directly related to the General Data Protection Regulation (GDPR), a law passed by the European Union in 2016. The GDPR deals with the privacy involved with data collection and its protection for the citizens of the European Union. This law gives citizens control over personal data that has been collected and published about them.

Due to the global notoriety of recent legal trials, coupled with the rising belief that people should have a say in what is posted about them online, this concept of the right to be forgotten is starting to gain headway in the United States. Further discussions of this as a natural human right will be faced in the future, and the outcome has the potential to impact the world beyond what can be imagined today.

**Case Study 6**

The Trolley Problem – Self-Driving Cars

With the massive acceleration of technology over the past 15 years, self-driving cars are no longer a dream of the past. With the promise of preventing wrecks that are most often caused by human error and allowing all car passengers to not be required to focus on the road, self-driving cars seem like a win in every aspect. While it is true that computers make drastically less mistakes than humans, accidents will still happen. This can even be seen in airplanes now, which are self-driving in many senses. Large programs like that largely cannot be without bugs. Aside from code errors, there are still humans involved in other environments that can cause problems for self-driving cars, which is where we see a few variations of the trolley problem.

The trolley problem can be boiled down to the debate between utilitarianism and deontological ethics. The dilemma presented in the trolley problem is as follows – you see a trolley headed for five people tied to its track who will surely be killed if they are hit. You have the option to change the trolley’s track, but the other track has one person tied to it. You must make a choice: either do nothing and five are killed, or act and one person is killed.

The self-driving car variation I would like to explore is one like the following. The self-driving car senses a group of children is playing in the street of a city. If the car takes no extra action, it will kill the children. However, if it decides to swerve, it will hit a pedestrian walking on the sidewalk. Should the self-driving car hit the children or swerve and take an extra part in hitting the pedestrian? The utilitarian would view would assert that it is the moral obligation of the self-driving car developers to swerve. The deontologist would argue swerving would cause unnecessary participation in the death of the pedestrian.

**Case Study 7**

Justina was a normal 15-year old kid who began experiencing weird symptoms and pain in her stomach. Her parents took her to a doctor and she was diagnosed with a rare mitochondrial disease. Later, at home, Justina was in so much pain, her parents rushed her off Boston’s Children's Hospital. The hospital told the parent that the illness and pain Justina was feeling was, in fact, all in her head. The doctors wanted to take Justina off of all her medication. When the parents refused, the doctors issued emergency custody of Justina under suspicion of medical child abuse. Justina was taken to the hospitals psych ward and only permitted to see her parents once a week, and a 20-min supervised phone call per day.

Justina’s parents went to local news and went public with their side of the story. This eventually went viral with an online campaign, soliciting volunteers to help spread the word. Protestors lined up outside Boston Medical Hospital. Tension was high and the hospital refused to release Justina. Justina’s parents then suffered from a gag order from the court, and were no longer allowed to speak out about Justina’s story. It looked like Justina would never be released back to her parents.

Martin Gottesfeld, a 30-year old computer security expert, saw the news and decided to act. During one of the hospital's biggest fundraising periods of the year, Gottesfeld attacked the computer servers of Children’s Hospital, Wayside Youth, and Family Support Network, all places where Justina had been kept. This DDoS attack lasted several days and estimated costs added up to roughly $600,000. Gottesfeld didn’t steal any information, or even look at any customer information. After investigation, Gottesfeld was arrested.

Gottesfeld states this as an act of digital protest to help raises awareness to Justina’s story and inevitably help with the release of Justina. Some view his attack as a reckless endangerment to everyone in the multiple hospitals and overall morally wicked. Eventually, Justina was released back to her parents, after 18 months of being kept away.

**Case Study 8**

When a computer crime is committed and the perpetrator is caught, they are usually charged with a standard crime alongside one for misusing a computer; in most cases, this is what happens to people who are in possession of stolen data. These rules usually have exceptions, and this is one of those cases – websites like <https://www.haveibeenpwned.com/> and <https://www.weleakinfo.com/> possess databases of information that have been stolen from other websites. These services are hosted under the guise that access to information should be free, so they can possess the data and display it to users. The two websites are different in the way that they display the data, and I will talk about this more in detail in the next two paragraphs.

The first website, haveibeenpwned, is a website that will allow you to search for specific email addresses through a list of breached sites. It will return what breached websites your email was shown in, so that you can hopefully use it to secure yourself. Breached websites are any websites that have had the database(s) holding sensitive information released to the public; these usually contain usernames, email addresses, IP addresses, passwords, and other sensitive information. The catch on this website is that it will merely display what websites your email was found in; it *will not* show you what information was stored in those websites. This is arguably done to prevent attackers from discovering your information, but the problem is that attackers *can* get this information if they need it. By merely masking the data, all it is doing is causing attackers to have to use a different service to discover that information (which is a rather easy task).

The second website, weleakinfo, is a website that will allow you to search for a variety of things: email addresses, usernames, passwords, hashes, IP addresses, names, phone numbers, or even specific website domains! The catch here is that this website *will* return the specific results that are stored within the databases. This means that entries containing sensitive information on you is accessible to strangers for a small amount of money per month! These services exist all over the internet and might seem very scary at first, but ultimately have their own good uses as well. Internet vigilantes use these services all the time to reveal information on criminals and missing/unidentified people, and government employees use these types of services as well. Some people even use these services to strengthen their own security; by seeing the specific information stored in websites, they can figure out which things are visible to the world and need to be changed/secured.

These services are offered on the surface of the Internet, for everybody to use and discover. This means ordinary teenagers can discover social security numbers and credit cards in your name with just a few clicks. While this shocking information is sure to frighten people, the good news is that it helps people everywhere. Seeing the dumped data can help researchers determine which passwords are used the most frequently (and can therefore block them being used on websites in the future) and help people make smarter decisions with their data footprints. This is also used so that websites can understand why it’s important to safeguard their user data. Unfortunately, breaches happen daily, but there is a lot we can do to prevent them. Using password storage software like KeePass can help you use a randomly generated password for each website and manage them all with one single secure password that you know. This stops attackers from being able to use these services to target specific individuals and helps strengthen Internet security at the same time. This combined with good Internet safety practices can help users stay safe from data breaches and attackers.

**Case Study 9**

The Unite the Right rally took place in Charlottesville, Virginia, between August 11th and 12th, 2017. The goal of this rally was to oppose the removal of the General Robert E. Lee statue located in Charlottesville’s Lee Park and to further unify the White Nationalist Movement. On August 11th, roughly 250 white nationalists and white supremacist marched through the University of Virginia campus. Bearing tiki torches, men and women shouted racist and antisemitic slogans including: “Blood and Soil!” and “Jews will not replace us!” Charlottesville then-mayor, Mike Signer, described the event as a, “Cowardly parade of hatred, bigotry, racism, and intolerance.” On August 12th, hundreds of white nationalist protestors gathered at Lee Park. Some carried signs and banners with references to the Nazi Party and the Ku Klux Klan, some waved Confederate flags, and others wore bright red “Make America Great Again” hats. Both the march and the rally ended in violence between white nationalist protestors and counter-protestors, forcing Virginia into a state of emergency. Protestors threw punches, chucked water bottles, exploded smoke bombs, and released chemical sprays. Following the failed rally, a vehicle drove into a crowd of counter-protesters, killing 32-year-old Heather Heyer and injuring more than a dozen others.

In response to the events, an activist took to Twitter, posting photographs and videos of the rally, in an effort to identify the white nationalists participating. Many participants were quickly identified. Two participants were separated from their employers, one voluntarily and the other involuntarily. Another was denounced by family members.

**Case Study 10**

The topic of this Case Study will focus on data mining, that is harvesting social media data to target advertisements to them. This case study will delve into the now infamous topic that is the Cambridge-Analytica scandal, detailing the major ethical issues that pertain to the topic. Being 5 years after the beginnings of this scandal, we now have access to the majority of all the information that has been surfacing throughout the years.

In this scandal, data company Cambridge Analytica is reported to have illegally accessed and modeled user data on the social media network, Facebook. The height of this began around two years before the United States’ presidential election was to take place. The company, supported by multiple Republican presidential candidates, including Ben Carson, Ted Cruz, and Donald Trump, accessed users’ data via an online questionnaire that required giving access to the user’s Facebook profile by paying them about one dollar. Information gathered from this included their demographic data friends lists, posts, and most importantly, “likes”.

Likes on Facebook are particularly important because the social network itself already places heavy emphasis on content you like to tailor your newsfeed and internal advertisements to what you would most likely relate or interact with. The users that participated in this online questionnaire also gave the company access to each of their friends and the friends’ data. This turned allowed what was about ten thousand original users’ data being accessed to grow exponentially. The data collected was then used to model each user’s personality based on the “big-five” personality traits. In turn, the company used the linked models to target specific campaign advertisements to users of particular demographics and personality types. Republican candidates used this information to gain voters and influence voters choices. Furthermore, the scandal goes beyond American politics; the company is also responsible for influencing Brexit voters in the United Kingdom.