**MIS 310 Week 11 Homework (30 points)** Name: Megan Leonard

You will not be given credit for answers that are copies or near verbatim transcripts – please use your own words and document sources where appropriate using proper APA guidelines. Apply the principles learned in this chapter (chapter 10) or previous chapters to answer the questions for this assignment.

**Chapter 10 Learning Outcomes**

|  |
| --- |
| * Describe some examples of waste and mistakes in an IS environment, their causes, and possible solutions. * Identify policies and procedures useful in eliminating waste and mistakes. * Discuss the principles and limits of an individual’s right to privacy. * Discuss the tradeoffs between security and privacy. * List the important negative effects of computers on the work environment. * Identify specific actions that must be taken to ensure the health and safety of employees. * Outline a process for including ethical considerations in decision making. * Define the intent and key elements of an effective code of ethics. |

**Week 11 Review Questions (10 points)**

Answer the following questions in one or more paragraphs using proper APA format as required**:**

1. [2 points] What issues and problems are raised by the use of unintegrated information systems?

Issues raised by using unintegrated information systems include difficulty with collaboration missed opportunities, leading to an increase in costs and potential loss of sales.

1. [2 points] What is ergonomics? How can it be applied to office workers?

Ergonomics involves the design of machines and how they can be made the safest and most efficient. This can be applied to office workers as making the systems the safest and most efficient will be able to help the workers complete their jobs with less difficulty.

1. [2 points] Provide a few examples of actions organizations are taking to help eliminate workers’ nonproductive computer-related activity.

A few actions organizations are taking to help eliminate workers’ nonproductive computer-related activity are putting in place workplace policies that the workers are trained in and then monitored to determine where nonproductive activity is done and where it needs help.

1. [2 points] What is the First Amendment? What is the Fourth Amendment? What rights do they guarantee?

The First Amendment is on the freedom of speech, religion, press, and the right to assemble. This guarantees that a person can speak their opinion without the fear on imprisonment. The Fourth Amendment is the right for a person to feel secure and not be unreasonably searched or have their possessions seized without a warrant. This lets a person feel safe in their own home without fear of unreasonable searches.

1. [2 points] What is meant by “reasonable expectation of privacy”? How does this impact the application of the Fourth Amendment?

The reasonable expectation of privacy means that a person can within the privacy of their space be able to do something without having someone listening or looking in on them. This impacts the Fourth Amendment as a means of if a person taps their phone or spies on them while they are in that privacy then they cannot be held without difficulty for their actions and words inside their home due to breaches of privacy.

**Week 11 Critical Thinking Exercise (10 points)**

Read the following and answer the questions in one or more paragraphs using proper APA format as required**:**

***Seeking Greater Customer Acceptance***

*Your organization has been in business over 10 years selling consumer home products over the Internet. A year ago, the firm gained much negative publicity when it was uncovered that the personal data it gathered was being sold, unknown to its customers, to third parties. The result was over a 15 percent drop in sales. At this time, the firm has no privacy policy and is debating whether to create such a policy, and if so, what terms it should include.*

1. [2 points] What is the purpose and intent of a privacy policy?

The purpose and intent of a privacy policy is to lay out what information is collected from the customers, how its used, and how the information is kept safe and secure. The intent is to reassure customers that any information they input will be safe and secure and kept private without the fear of the information being sold or leaked. Any information that would be sent to third parties would be basic information and stated to show the intention the company has with the data.

1. [2 points] What are the key elements that need to be included in an effective privacy policy?

Key elements that are included in a privacy policy would be intent on what information is collected, what would be shared, what is to be kept private and secure, why certain information is needed, and how the company uses the information they are given.

1. [3 points] What obligations and potential issues are raised by creating a privacy policy?

Potential issues raised by the privacy policy is that the information they gather is told so if a hacker wanted a credit card, they could see that the information for the card is saved by the company. It also lays specific intents that if broken for any reason could lead to the company being sued by all the customers and loosing.

1. [3 points] What measures should be taken to avoid potential litigation over any new privacy policy?

Measures to be taken to avoid problems would be to increase their security and how they keep the information. For instance if they save the credit card number, they could save the first half but require the customer to fill in the cvv and the last four digits on the card.

**Week 11 Case Study (10 points)**

Read the following and answer the questions in one or more paragraphs using proper APA format as required**:**

***FBI Orders Apple to Unlock iPhone***

*On December 2, 2015, Syed Rizwan Farook and Tashfeen Malik burst into a holiday gathering of county employees at the Inland Regional Center in San Bernardino, California, and began shooting—ultimately killing 14 people and wounding another 21. In the hours after the attack, the couple became involved in a shootout with police, and both were killed.*

*With their deaths, the investigation into the deadliest terrorist attack in the United States since September 11, 2001, entered a new phase, as hundreds of FBI agents in California and around the world began investigating the attackers’ online and offline activities in the hours, weeks, and months leading up to the shootings. In addition to the stockpile of weapons and homemade pipe bombs found in the home of Farook and Malik, investigators found multiple electronic devices. While attempts had been made by the couple to delete data and damage some of the devices, FBI Director James Comey reported two weeks after the attack that investigators had found private messages between the two that showed their “joint commitment to jihad and to martyrdom.” In addition, Malik posted a note on Facebook shortly after the shootings, pledging the couple’s allegiance to the leader of ISIS, a terrorist network also known as the Islamic State.*

*In order to further investigate possible connections to extremist groups, the FBI attempted to access the data on an iPhone used by Farook. The phone, which belonged to Farook’s employer, the San Bernardino County Health Department, was locked by a passcode, and neither the county nor the FBI were able to unlock the phone. The iOS software installed on Apple’s phones allows only 10 unsuccessful passcode attempts before it wipes the phone’s memory clean. This security feature prevented the FBI from attempting a “brute-force” attack, which is essentially a trial-and-error method in which all possible passcodes are tried systematically until the correct one is uncovered.*

*In the weeks following the shootings, Apple representatives cooperated with the FBI’s investigation, providing some older data backups from the phone as well as suggesting possible methods the agency could use to access the data on the phone itself. The company balked, however, when the FBI demanded that the company develop new software that would disable the functionality that wipes the phone’s memory when too many wrong passcodes are entered in a row. The FBI also wanted Apple to eliminate the built-in delay between passcode attempts, which, by Apple’s estimates, meant that a brute-force attack on a phone with a six-digit passcode could take more than five years to complete.*

*The FBI’s demand that Apple develop new software that would allow it to unlock the phone in this case is an extension of an ongoing debate about whether tech companies should be compelled to build a “backdoor” into their software that would allow the government to access data even when secure encryption has been used to protect it. Without it, some law enforcement experts warn, the United States could be faced with the prospect of what has been dubbed the “Going Dark” problem, which some experts fear would lead to the inability of law enforcement to access electronic data even with a warrant. That concern was heightened for some when Apple announced in 2014 that it had altered its software so that it was no longer “technically feasible for us to respond to government warrants for the extraction of data from devices” running iOS 8 or later versions of that software.*

*On February 16, 2016, a U.S. magistrate in California ordered Apple to assist the government by creating a custom version of iOS that would run only on the iPhone in question and that would provide the functionality demanded by the FBI. In its motion requesting the order, the Department of Justice cited the All Writs Act, a law signed by President George Washington, which, among other things, gives federal judges the power to issue court orders compelling people to do things within the limits of the law and which has frequently been used as the basis for court orders compelling telecommunications companies to install and**operate call-tracking devices. In its filing, the DOJ alleged that Apple “deliberately raised technological barriers that now stand between a lawful warrant and an iPhone containing evidence related to the terrorist mass murder of 14 Americans.”*

*Apple challenged the judge’s order, arguing that it would set dangerous legal precedent. The company also issued a statement on its Web site that said, in part, “The implications of the government’s demands are chilling. 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 to intercept your messages, access your health records or financial data, track your location, or even access your phone’s microphone or camera without your knowledge.” According to Apple, “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.”*

*The case took another turn before the scheduled court hearing on the issue in March 2016, when the Justice Department announced that it had successfully accessed the contents of the phone using a tool provided the government by an unnamed third party. After its announcement, the Justice Department withdrew its motion to compel Apple to develop the requested software; however, according to a Justice Department spokeswoman, “It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety, either with cooperation from relevant parties, or through the court system when cooperation fails.”*

1. [3 points] Why did Apple object to the court order in this case? What was the government’s rationale for compelling Apply to comply with the order?

Apple objected the court order in this case because what the government is asking them to do would be a breach in their customer’s privacy and lead to trouble for the company. The government believed that they would be able to use the backdoor to stop future threats of terrorists and the outcome would be greater than the means.

1. [3 points] Do you think Americans should be willing to surrender some of their privacy for increased security by allowing backdoors that enable law enforcement access to smartphones and other devices after a search warrant has been issued? Why or why not?

No, because the privacy of our online activity is very important as most of what we do is now online. The government may not think of the context of conversations before trying to arrest someone based off a conversation they have with a friend on their phone or messages. For instance, Call of Duty is a shooter game that a lot of people play or have discussions on. Two friends who play the game together could have a full conversation about their kill count or strategies for shooting others without needing to state the game, knowing that they are talking about the game. With the backdoor, the government could see this conversation and then go after these two thinking it is a threat when in reality it is just two twelve-year-old kids who like shooter games. The back door causes a lot of problems for the average person as there are thousands of people to the one terrorist and the back door is not a guarantee that the people would be safe.

1. [4 points] The FBI and Apple are involved in similar disputes in other cases, including one in New York involving an alleged drug conspiracy. Shortly before the government dropped its legal action against Apple in the San Bernardino case, the judge in the New York case ruled against the government, rejecting the argument that the All Writs Act gave prosecutors the authority to compel Apple to bypass the lock on the seized phone. Do your opinions about the issues involved in the San Bernardino case change when they arise in connection with a case that does not have national security implications? Why or why not?

My opinion does not change as I believe that the back door is dangerous in many different means. I am an avid player of GTA V and when I talk to my friends in game or while I am playing I do not focus on stating that I am playing a game each time I talk about using a rocket launcher as my friends understand that I am playing and not doing something illegal. If the government makes Apple make a backdoor then their systems would not be as secure and could allow hackers to break through and access their users. By creating a hole in the wall for one person, there is always the chance that others will come through when the hole only has wire covering it.

SOURCES: Almasy, Steve, “FBI Asks for Help Filling in San Bernardino Terrorist Attack Timeline,” CNN, January 5, 2016, www.cnn.com/2016/01/05/us/san-bernardino-terrorist-attack; Nelson, Joe, “Investigation into San Bernardino Mass Shooting Will Be ‘Expansive and Expensive’,” San Bernardino County Sun, www.sbsun.com/general-news/20151220/investigation-into-san-bernardino-mass-shooting-will-be-expansive-and-expensive; Medina, Jennifer, Richard Perez-Pena, Michael S. Schmidt, and Laurie Goldstein, “San Bernardino Suspects Left Trail of Clues, but No Clear Motive,” New York Times, December 3, 2015, www.nytimes.com/2015/12/04/us/san-bernardino-shooting.html?\_r=0; Goldman, Adam and Mark Berman, “FBI: San Bernardino Attackers Didn’t Show Public Support for Jihad On Social Media,” Washington Post, December 16, 2015, www.washingtonpost.com/news/post-nation/wp/2015/12/16/fbi-san-bernardino-attackers-didnt-show-public-support-for-jihad-on-social-media; Green, Chloe, “Brute Force Attacks: How You Can Stop Hackers Breaking Your Door In,” Information Age, May 11, 2016, www.information-age.com/technology/security/123461414/brute-force-attacks-how-you-can-stop-hackers-breaking-your-door; “Operational Technology: Going Dark Issue,” Federal Bureau of Investigation, www.fbi.gov/about-us/otd/going-dark-issue, accessed May 9, 2016; Panzarino, Matthew, “No, Apple Has Not Unlocked 70 iPhones for Law Enforcement,” TechCrunch, February 18, 2016, http://techcrunch.com/2016/02/18/no-apple-has-not-unlocked-70-iphones-for-law-enforcement; Palazzolo, Joe and Devlin Barrett, “Roots of Apple-FBI Standoff Reach Back to 2008 Case,” Wall Street Journal, www.wsj.com/articles/roots-of-apple-fbi-standoff-reach-back-to-2008-case-1460052008?mg=id-wsj; Timberg, Craig, “Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants,” Washington Post, September 18, 2014, www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f\_story.html; Lewis, Danny, “What the All Writs Act of 1789 Has to Do with the iPhone,” Smithsonian, February 24, 2016, www.smithsonianmag.com/smart-news/what-all-writs-act-1789-has-do-iphone-180958188/?no-ist; Hollister, Sean and Connie Guglielmo, “How an iPhone Became the FBI’s Public Enemy No. 1 (FAQ),” CNET, February 25, 2016, www.cnet.com/news/apple-versus-the-fbi-why-the-lowest-priced-iphone-has-the-us-in-a-tizzy-faq; “A Message to Our Customers,” Apple, February 16, 2016, www.apple.com/customer-letter; Barrett, Devlin, “FBI Paid More than $1 Million to Hack San Bernardino iPhone,” Wall Street Journal, April 21, 2016, www.wsj.com/articles/comey-fbi-paid-more-than-1-million-to-hack-san-bernardino-iphone-1461266641; Zetter, Kim, “Apple’s FBI Battle Is Complicated. Here’s What’s Really Going On,” Wired, February 18, 2016, www.wired.com/2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on; Barrett, Devlin, “Judge Sides with Apple in N.Y. Drug Case Involving Locked Phone,” Wall Street Journal, March 1, 2016, [www.wsj.com/articles/judge-sides-with-apple-in-drug-case-involving-locked-phone-1456785910](http://www.wsj.com/articles/judge-sides-with-apple-in-drug-case-involving-locked-phone-1456785910).