

PGDM, 2020-22
Information Systems Management for Business
DM-103
Trimester – I, End-Term Examination: October 2020

Time allowed: 2 Hrs 30 Min
Max Marks: 50

Roll No: _____

Instruction: Students are required to write Roll No on every page of the question paper, writing anything except the Roll No will be treated as **Unfair Means**. All other instructions on the reverse of Admit Card should be followed meticulously.

Sections	No. of Questions to attempt	Marks	Total Marks
A	Attempt 2 long questions (from internal choices given in question 1 and 2) Or Attempt 2 short questions (from internal choices given in question 3 and 4)	2*10 Or 2*5	20 10
B	Compulsory Case Study with minimum of 2 questions	20	20
			50

SECTION-A

Long Answers – 2X10 marks

1 A. Describe how e-commerce has brought transformation in following industries

- Books
- Music
- Air Travel
- Movies
- Real estate
- Bill Payment
- Software
- Tourism
- Insurance
- Education

CILO 3

OR

1B. Explain how social networking and the “wisdom of crowds” help companies improve their marketing. **CILO 3**

- 2A. Select any company (a public sector bank, an insurance firm, a large retail store, or a national telecom service provider) and answer the questions given below
- Does this company need data warehousing or data mining and for what benefits
 - What typical possible patterns would you like to extract by data mining

CILO2

OR

2B. Toronto based Mercedes-Benz Canada, with a network of 55 dealers, did not know enough about its customers. Dealers provided customer data to the company on an ad hoc basis. Mercedes did not force dealers to report this information. There was no real incentive for dealers to share information with the company. How could CRM and PRM system help solve this problem? **CILO 2**

Short Answers - 2X5 marks

3A. Should producers of software based services, such as ATMs, be held responsible for economic damages suffered from their system failures? **CILO4**

OR

3B. List and describe the key technological trends that heighten ethical concerns. **CILO4**

4A. Describe how promoting synergies and core competencies enhances competitive advantage. **CILO 1**

OR

4B. Supply chain management is less about managing the physical movement of goods and more about managing information. Discuss the implications of this statement. **CILO 1**

SECTION-B

Compulsory Case Study – 20 Marks

Apple Inc. vs FBI

San Benadino, California saw one of the deadliest shootings on December 2, 2015, killing 14 and injuring 22 people. Federal Bureau of Investigation (FBI) found three phones when searched the house of the couple. Over a period of next few months, FBI tried to access all the data they could from the phone with the help of Apple Inc. that provided all the information they had on account back up system. However, FBI were not able to unlock the phone that required a four-digit passcode which after 10 wrong tries would erase all the data. The FBI asked Apple to design a system to bypass the 10-try limit so that they could access the phone data by trying all the possible actions. Apple, however, declined to create such a programme. This move was publicly supported by tech companies like Yahoo! and Facebook. The UN human rights chief urged US authorities to proceed with caution as it may have “extremely damaging implications”ⁱ on human rights, journalists, political dissidents and others. On the other hand, the families of victims and survivors criticized Apple’s move expressing their concerns over obstacles for the investigation.

President Obama embraced the law enforcement position stating “law enforcement must be legally able to collect information from smartphones and other electronic devices”ⁱⁱ.

This dispute between Apple Inc. and FBI has brought forward the tension between privacy and national security. On February 16, 2016, the company published a details statement on their website clarifying why it did not comply with the request made by FBI.

February 16, 2016

A message to our customers

<https://www.apple.com/customer-letter/>

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand. This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

The Need for Encryption

Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our notes, our calendars and contacts, our financial information and health data, even where we have been and where we are going.

All that information needs to be protected from hackers and criminals who want to access it, steal it, and use it without our knowledge or permission. Customers expect Apple and other technology companies to do everything in our power to protect their personal information, and at Apple we are deeply committed to safeguarding their data.

Compromising the security of our personal information can ultimately put our personal safety at risk. That is why encryption has become so important to all of us.

For many years, we have used encryption to protect our customers’ personal data because we believe it’s the only way to keep their information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business.

The San Bernardino Case

We were shocked and outraged by the deadly act of terrorism in San Bernardino last December. We mourn the loss of life and want justice for all those whose lives were affected. The FBI asked us for help in the days following the attack, and we have worked hard to support the government’s efforts to solve this horrible crime. We have no sympathy for terrorists.

When the FBI has requested data that's in our possession, we have provided it. Apple complies with valid subpoenas and search warrants, as we have in the San Bernardino case. We have also made Apple engineers available to advise the FBI, and we've offered our best ideas on a number of investigative options at their disposal.

We have great respect for the professionals at the FBI, and we believe their intentions are good. 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.

Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.

The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.

The Threat to Data Security

Some would argue that building a backdoor for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case.

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and it is only as secure as the protections around it. Once the information is known, or a way to bypass the code is revealed, the encryption can be defeated by anyone with that knowledge.

The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.

The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.

We can find no precedent for an American company being forced to expose its customers to a greater risk of attack. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.

A Dangerous Precedent

Rather than asking for legislative action through Congress, the FBI is proposing an unprecedented use of the All Writs Act of 1789 to justify an expansion of its authority.

The government would have us remove security features and add new capabilities to the operating system, allowing a passcode to be input electronically. This would make it easier to unlock an iPhone by “brute force,” trying thousands or millions of combinations with the speed of a modern computer.

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.

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.

We are challenging the FBI’s demands with the deepest respect for American democracy and a love of our country. We believe it would be in the best interest of everyone to step back and consider the implications.

While we believe the FBI’s intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect.

Questions

CILO 3

1. What are the potential harms by :
 - a. FBI’s demand that Apple help it open an iPhone
 - b. Apple’s refusal to help the FBI
2. Did Apple have a moral obligation to help FBI to access the iPhone in this case? What if it involved a different type of criminal activity such as drug trafficking? Explain your reasoning.
3. Apple argued that helping FBI access the iPhone would produce code that would make private information on all iPhones vulnerable, not only to the American Government but also to other foreign governments and criminal elements. Does avoiding these harms provide adequate justification for Apple’s refusal to open the phone?
4. Politicians from across the political spectrum, including President Obama argued that the technology preventing government access to information should not exist. Do you agree with this limit on personal privacy? Why or Why not?

ⁱ Associated Press, “The UN human rights chief says U.S. authorities ‘risk unlocking a Pandora’s Box’ in their efforts to force Apple to create software to crack the security features on its phones, and is urging them to proceed with caution,” *U. S. News and World Report*, Mar. 4, 2016, <http://www.usnews.com/news/technology/articles/2016-03-04/un-human-rights-chief-warns-of-implications-of-apple-fbi-row>.

ⁱⁱ New York Times, “Obama, at South by Southwest, Calls for Law Enforcement Access in Encryption Fight”, March 11, 2016, <https://www.nytimes.com/2016/03/12/us/politics/obama-heads-to-south-by-southwest-festival-to-talk-about-technology.html>