PGDM (IBM), 2018-20
IT in Insurance
INS- 105
Trimester – I, End-Term Examination: September 2018

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.

Sec A
Attempt any 3 out of 5 Questions   **3*5 = 15 Marks**

1. What are the management, organization and technology components of an information system?
2. Describe the five steps in an ethical analysis.
3. Describe the pros and cons of allowing companies to amass personal data for behavioural targeting.
4. Describe the role of information policy and data administration in information management.
5. The internet may not make corporations obsolete, but the corporations will have to change their business models. Do you agree? Why or why not?

Sec B
Attempt any 2 out of 3 Questions   **2*10= 20 Marks**

1. Describe four competitive strategies enabled by information systems that firms can pursue.
2. Choose any emerging technology (AI, IoT, Block chain, AR/ VR, Geoservices, Wearable technology …… etc.) and develop a service for insurance industry. Describe the role of management, organization and technology in developing such a service.
3. For an insurance company that has a website and accepts payment, discuss the major security threats to their website and its potential impact. What can be done to minimize these threats?

SEC C
Case study   **15 Marks**

Big Data Gets Personal: Behavioral Targeting

Ever get the feeling somebody is trailing you on the Web, watching your every click? Do you wonder why you start seeing display ads and pop-ups just after you've been searching the Web for a car, a dress, or cosmetic product? Well, you're right: your behavior is being tracked, and you are being targeted on the Web as you move from site to site in order to expose you to certain "targeted" ads. It's Big Data's dark side.

13

Individual Web sites and companies whose business is identifying and tracking Internet users for advertisers and marketers are collecting data on your every online move. Google, which handles more than 3.5 billion Web searches each day, knows more about you than your mother does. Many of the tracking tools gather incredibly personal information such as age, gender, race, income, marital status, health concerns (health topics you search on), TV shows and movies viewed, magazines and newspapers read, and books purchased. A $31 billion dollar online ad industry is driving this intense data collection. Facebook, which maintains detailed data on over I billion users, employs it's Like button to follow users around the Web even if you log off. Its social networking site is one giant tracking system that remembers what you like, what your friends like, and whatever you reveal on your Wall. (See the chapter-ending case study.) Plus, Google's social networking tool, knows about your friendships on Gmail, the places you go on maps, and how you spend your time on the more than two million websites in Google's ad network. It is able to gather this information even though relatively few people use Plus for their social network.

While tracking firms claim the information they gather is anonymous, this is true in name only. Scholars have shown that with just a few pieces of information, such as age, gender, zip code, and marital status, specific individuals can be easily identified. Moreover, tracking firms combine their online data with data they purchase from offline firms who track retail store purchases of virtually all Americans. Here, personal names and other identifiers are used.

Use of real identities across the Web is going mainstream at a rapid clip. A Wall Street Journal examination of nearly 1,000 top Websites found that 75% now include code from social networks, such as Facebook's "Like" or Twitters "Tweet" buttons. Such code can match people's identities with their Web-browsing activities on an unprecedented scale and can even track a user's arrival on a page if the button is never clicked.

In separate research, the Journal examined. What happens when people logged in to roughly 70 popular Websites that request a login and found that more than a quarter of the time, the sites passed along a user's real name, email address or other personal details to third-party companies.

Online advertising titans like Google, Microsoft, and Yahoo are all looking for ways to monetize their huge collections of online behavioral data. While search engine marketing is arguably the most effective form of advertising in history, untargeted banner display ad marketing is highly inefficient because it displays ads to everyone regardless of their interests. As a result, these firms cannot charge much for display ads. However, by tracking the online movements of 245 million U.S. Internet users, they can develop a very clear picture of who you are, and use that information to show you ads that might be of interest to you. This would make the marketing process more efficient, and more profitable for all the parties involved.

You're also being tracked closely when you use your mobile phone to access the Internet, visit your Facebook page, get Twitter feeds, Watch video, and listen to music. The mobile Web is working hard to keep track of your whereabouts, locations, habits, and friends in the hope of selling you even more products and services.

New technologies found on smartphones can identify where you are located within a few yards. Performing routine actions using your smart phone makes it possible to locate you throughout the day, to report this information to corporate databases, retain and analyze the

information, and then sell it to advertisers. Most of the popular apps report your location. Law enforcement agencies certainly have an interest in knowing the whereabouts of criminals and suspects. There are, of course, many times when you would like to report your location either automatically or on your command. If you were injured, for instance, you might like your cell phone to be able to automatically report your location to authorities, on if you were in a restaurant, you might want to notify your friends where you are and what you are doing. But what about occasions when you don't want anyone to know where you are, least of all advertisers and marketers?

Location data gathered from cell phones has extraordinary commercial value because advertising companies can send you highly targeted advertisements, coupons, and flash bargains, based on where you are located. This technology is the foundation for many location-based services, which include smartphone maps and charts, shopping apps, and social apps that you can use to let your friends know where you are and what you are doing. Revenues from the global location-based services market are projected to reach $10.3 billion in 2015, according to Gartner.

Both Apple's iPhone and Google's Android phones collect personal, private location data, and both firms are building massive databases that can pinpoint your location. Advertising firms pay Apple and Google for that information and for distributing their mobile ads, and they are becoming increasingly important sources of revenue. In 2012, Google earned $2.2 billion from its mobile ads. Smartphone apps that provide location-based services are also sources of personal, private location information based on the smartphone GPS capability.

Expect those eyes to follow your movements even more in the future as behavioural targeting becomes even more precise. New software is being developed to help advertisers track users across devices by establishing cross-screen identities. That means that companies will be able to serve ads to your mobile phone based on what they learned about you from surfing the Web on your PC.

QUESTIONS   3*5= 15 Marks

1. Why is behavioural tracking such an important ethical dilemma today? Identify the stakeholders and interest groups in favour of and opposed to behavioral.
2. How do businesses benefit from behavioural tracking? Do people benefit? Explain your answer.
3. What would happen if there were no behavioural tracking on the Internet?