

Name: _____

USC ID: _____

INF 529 Midterm Exam

Spring 2020

IMPORTANT: FOR REMOTE PROCTORS

Please Scan Both Sides of all Pages
Students have been instructed to answer
some questions on the back of the page.

Instructions:

Show all work. This exam is open book and open note. You may use electronic devices to consult materials stored on the devices, but you may not use them to access material through the net, or for communication in any manner. Electronic devices must be placed in “airplane mode” with wifi and other communications capabilities disabled. You have **100 minutes** to complete the exam.

Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. **Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question.** The exam will be split apart for grading by different people, and if part of your answer for one question appears on a page given to a different grade because the sheet contains parts of the answer to more than one question, then you will NOT receive credit for that part of the answer not seen by the grader. In particular, **each numbered question must appear on separate pieces of paper so that the exam can be split for grading.**

Be sure to include your **name on each page.**

There are **100 points** in all and **3 questions.**

	Q1	Q2	Q3		Total Score
Score					

Name: _____

USC ID: _____

1) Expectations of Privacy (30 points)

Although intended by US courts to apply to governments' access to business records, the "third party doctrine" is actually a very accurate statement of what happens to our data today when we provide the data to third parties. Although privacy regulations and communicated privacy policies may tell us otherwise, there is always the danger (and expectation) that our data will get out if we provide it to third parties. In this question I am concerned with our **actual** expectation of privacy, specifically with respect to whom our information may be provided (including for government and commercial purposes) and how it may be used.

- a) List some data (or actions that you might take) that leave you with zero expectations of privacy with respect to the data you have provided. For some of the examples of this "non-private" data, can you think of examples of ways that we expect the data should not be used. (10 points)

- b) Explain some of the changes to technology that have resulted in the disclosure of data that is 'non-private' (i.e. in plain view) having a significant impact on our privacy when combined with similar data. (10 points – answer on back of page)

Name: _____

USC ID: _____

- c) Provide several examples (possibly from current events) where data that has been entrusted to a third party (and which is not in plain view) has been used in unexpected ways, violating the user's privacy expectations. (10 points)

Name: _____

USC ID: _____

- 2) The most common manner by which adversaries steal our personal data is through impersonation. When our data is stored on our local device, or on the servers of social media and cloud services, the data is supposed to be accessed only by authorized users. If an adversary can pose as a different user for the purpose of making requests, then they can use the privileges associated with the identity that has been impersonated. (30 points)
- a) List some of the ways that an adversary is able to make request posing as a different user. There are at least two significantly different ways that this can be accomplished. (10 points)

- b) What are some of the approaches by which you can mitigate the impact of such impersonation activities? (by mitigate, I specifically do NOT mean prevent the impersonation from occurring, what I mean is that you should take steps to ensure the least resulting impact when impersonation does occur). (10 points – answer on back of page)

Name: _____

USC ID: _____

- c) What are the three main approaches that computer systems can use to confirm identity (authentication). What are the tradeoffs between the different approaches and what steps can a system designer or an end user take to improve the effectiveness of the authentication process? (20 points)

(note that there are three questions in part c, be sure to answer all of them).

Name: _____

USC ID: _____

- 3) One definition of privacy discussed in class is that privacy is the right to be let alone. By its nature, social media is intrusive. In this question I want you to discuss some of the ways that social media is problematic for our security and privacy.
- a) When we use social media, we voluntarily provide information that reveals our most sensitive characteristics: our likes and dislikes, who our friends are (i.e. our social network itself), our daily schedule, planned travels, the food we eat, etc. Discuss some of the ways that this data is used (i.e. for the purposes that we choose to use these sites) and mis-used (how the sites use this data in ways that are not necessary to the benefit of the end-user, including ways that the user is “monetized”). (10 points)

- b) Discuss some ways that social media may be used to control us, i.e. how can it more effectively influence our actions and our speech than other media? Consider how it can also affect the actions and speech of those that are not actively using such social media platforms. Specifically consider the incentives and disincentives provided through the social media platform itself. (10 points – answer on back of page)

Name: _____

USC ID: _____

- c) Social media platforms touch many of our devices and our social media “timelines” are often integrated with our other internet connected activities. How does this integration with our “timeline” affect the privacy of the data associated with our other activities? (10 points)