RUTGERS
Rutgers Business School
Newark and New Brunswick

22:198:645:01: Data Privacy
Spring 2018
1 WP – 120, Newark
1:00 Pm – 3:50 PM

Dr. Jaideep Vaidya
1 WP - 1080
973-353-1441
jsvaidya@business.rutgers.edu
Office Hours: 12:00 – 1:00 PM and by appt

COURSE DESCRIPTION

New technology has increasingly enabled corporations and governments to collect and use huge amount of data related to individuals. At the same time, legitimate uses in healthcare, crime prevention and terrorism demand that collected information be shared by more people than most of us ever know. Today, the challenge is enabling the legitimate use of the collected data without violating privacy. From the organizational perspective, enabling safe and secure use of owned data can lead to great value addition and return on investment. In this course, we are going to analyze the legal and social aspects of privacy and explore potential tools, techniques and technologies that can enhance privacy.

Thus, you will learn the basic issues underlying privacy in computing today. We will consider the core issues surrounding privacy, security, data storage and analysis and the technologies that have been developed to address those issues. The plan is to understand the theoretical concept of secure computation, using data mining to give an application oriented view. We will look at the important regulations in force today including HIPAA, Sarbanes-Oxley, EU GDPR, etc. and consider what comprises compliance. We will see the benefits of information sharing, including managerial impacts, and how to enable it in a secure manner. At the end of the course, a student should know the state of the art in privacy preserving computation and be able to apply his/her knowledge to new research.

COURSE MATERIALS

- Textbook(s): There is no prescribed textbook. However, several books will be useful for specific topics. For differential privacy, the following book is useful: The Algorithmic Foundations of Differential Privacy, Cynthia Dwork and Aaron Roth. DOI: 10.1561/0400000042.
- Check Blackboard (blackboard.rutgers.edu) and your official Rutgers email account regularly.

LEARNING GOALS AND OBJECTIVES

- This course is designed to help students develop skills and knowledge in the following area(s):

1. Advanced Knowledge in Specialized Areas
2. Advanced Research Skills
3. Ethical Judgement

- Students who complete this course will demonstrate the following:

a. Students will develop advanced theoretical or practical research skills in the area of privacy.
b. Students will make original research contributions.

c. Doctoral students will complete dissertation proposals, an original intellectual contribution to their field of knowledge.

- Students develop these skills and knowledge through the following course activities and assignments:

Lectures, Homeworks, Exams, and Term project. Students will be asked to read assigned research papers, critique them, and present them. Students will also work on a term project in which they try to identify a new privacy problem and propose a novel solution or implement a solution for it. I fully expect to see publishable work proceeding from this. Projects can be done individually or as a group of two students. Your project should proceed in two phases:
1. Around the middle of the term, you should plan to present a preliminary project proposal.
2. At the end of the semester, you should give a presentation related to the outcome of your project, and submit a final project report.

After completing the course, students will be able to:
□ Become familiar with the basics of privacy.
□ Understand how privacy is formalized.
□ Understand the common data privacy techniques.

PREQUISITES

Undergraduate level knowledge in basic statistics and databases is needed.

ACADEMIC INTEGRITY

I do NOT *tolerate cheating*. Students are responsible for understanding the RU Academic Integrity Policy (http://academicintegrity.rutgers.edu/files/documents/AI_Policy_2013.pdf). I will strongly enforce this Policy and pursue *all* violations. On all examinations and assignments, students must sign the RU Honor Pledge, which states, "On my honor, I have neither received nor given any unauthorized assistance on this examination or assignment." [I will screen all written assignments through *SafeAssign* or *Turnitin*, plagiarism detection services that compare the work against a large database of past work.] Don't let cheating destroy your hard-earned opportunity to learn. See business.rutgers.edu/ai for more details.

ATTENDANCE AND PREPARATION POLICY

- Expect me to attend all class sessions. I expect the same of you. If I am to be absent, my department chair or I will send you notice via email and Blackboard as far in advance as possible. If you are to be absent, report your absence in advance at https://sims.rutgers.edu/ssra/. If your absence is due to religious observance, a Rutgers-approved activity, illness, or family emergency/death and you seek makeup work, also send me an email with full details and supporting documentation within a week of your first absence.

- For weather emergencies, consult the campus home page. If the campus is open, class will be held.

- Expect me to arrive on time for each class session. I expect the same of you.

- Expect me to remain for the entirety of each class session. I expect the same of you.

- Expect me to prepare properly for each class session. I expect the same of you. Complete all background reading and assignments. You cannot learn if you are not prepared. The minimum expectation is that for each 3-hour class session, you have prepared by studying for at least twice as many hours.

- Expect me to participate fully in each class session. I expect the same of you. Stay focused and involved. You cannot learn if you are not paying attention.

CLASSROOM CONDUCT

Students are responsible for reviewing the specified chapters covered by the lecture. Please note that you are responsible for the ENTIRE content of each chapter plus any additional handouts, unless otherwise notified. You are not allowed to possess, look at, use, or in any other way derive advantage from the solutions prepared in prior years, whether these solutions are former students' work or copies of solutions that were made available by instructors.

You should exchange ideas and engage in a class discussion for the topics (and related papers) discussed in class. Participation is graded, in the sense that informative comments are valued.

Electronic Devices: In order to minimize the level of distraction, all watches, beepers and cellular phones must be on quiet mode during class meeting times. Students who wish to use a computer/PDA for note taking need prior approval of the instructor since key clicks and other noises can distract other students. Recording of lectures by any method requires prior approval of the instructor.

Email Messages: Remember to put the course number (CIS645) in the subject field of every e-mail message that you send me. E-mail messages that are missing this information are likely to be automatically redirected to a folder the instructor will seldom check, and it is not our responsibility to respond to these.

EXAM DATES AND POLICIES

There are 2 exams in this course:

Midterm Exam: 03/01/2018. In class, and will cover material upto that point.
Final Exam: 05/03/2018. In Class, and will be comprehensive

During exams, the following rules apply:

- If you have a disability that influences testing procedures, provide me an official letter from the Office of Disability Services at the start of the semester.
- No cell phones or other electronics are allowed in the testing room.
- Alternate seating; do not sit next to another student or in your usual seat.
- Your exam will not be accepted unless you sign the Honor Pledge.

GRADING POLICY

Course grades are determined as follows:

- Midterm Exam: 25%
- Final Exam: 25%
- Assignments and Class Project: 30%

- Paper Presentation: 10%
- Class Participation: 10%

Note: There will be no extra credit assignments, quizzes, or exams. Therefore, please plan to put in your best effort right from the start. Your final grade is not subject to negotiation. If you feel I have made an error, submit your written argument to me within one week of receiving your final grade. Clarify the precise error I made and provide all due supporting documentation. If I have made an error, I will gladly correct it. But I will adjust grades only if I have made an error. I cannot and will not adjust grades based on consequences, such as hurt pride, lost scholarships, lost tuition reimbursement, lost job opportunities, or dismissals. Do not ask me to do so. It is dishonest to attempt to influence faculty in an effort to obtain a grade that you did not earn, and it will not work.

COURSE TOPICS (tentative)

Part I: Understanding Privacy
Social Aspects of Privacy
Legal Aspects of Privacy and Privacy Regulations
Effect of Database and Data Mining technologies on privacy
Privacy challenges raised by new emerging technologies such RFID, biometrics, etc.

Part II: Privacy Models
Anonymization models:
K-anonymity, l-diversity, t-closeness, differential privacy
Database as a service, cloud computing

Part III: Using technology for preserving privacy.
Statistical Database security
Inference Control
Secure Multi-party computation and Cryptography
Privacy-preserving Data mining
Hippocratic databases

Part IV: Emerging Applications
Social Network Privacy
Location Privacy
Query Log Privacy
Biomedical Privacy

COURSE SCHEDULE

Date Topic Items Due

Week 1 – 01/18/2018
We will go over the course topics and discuss the grading issues. We will also discuss background material for the course.

Week 2 (Legal aspects of privacy) – 01/25/2018
We will look at the legal aspects of privacy and laws pertaining to it. We will also look at how Google Searching can breach privacy.

Week 3 (Database privacy) – 02/01/2018
We will discuss database privacy models, including the classic k-anonymity model, l-diversity, t-closeness, and differential privacy.

Week 4 Differential Privacy – 02/08/2018
We will continue our discussion of differential privacy.

Week 5 (Statistical databases and query auditing) – 02/15/2018
We will continue our discussion of differential privacy, and look at privacy in statistical databases and query auditing. We will also look at the database as a service model, and issues in cloud computing.

Week 6 (Location privacy) – 02/22/2018
We will look at the problem with privacy in mobile environments and location privacy issues.

Week 7 – 03/01/2018
Midterm Exam

Week 7 (Cryptographic essentials) – 03/08/2018
We will briefly cover the basic cryptographic techniques as well provide an overview of Secure Multi-party Computation Techniques. Project preliminary presentations (10 mins each) are also due.

Week 8 (Privacy-preserving Data Mining) – 03/22/2018
We will look at the problems and techniques in privacy-preserving data mining.

Week 9 (Graph and social network privacy) – 03/29/2018
We will look at privacy problems in graph-structured data and consider the problem of social network privacy.

Week 10 (RFID privacy) – 04/05/2018
We will look at privacy issues in RFID devices.

Week 11 (Financial cryptography and cryptography for SCM) – 04/12/2018
We will look at Privacy-Preserving Transportation Logistics and Supply Chain Management and also some applications in financial cryptography.

Week 12 (Big data privacy) – 04/19/2018
We will look at the implications of big data on privacy.

Week 14 (Project Presentations) – 04/26/2018

Project Presentations

Week 15 – 05/03/2018
Final Exam

SUPPORT SERVICES

If you need accommodation for a *disability*, obtain a Letter of Accommodation from the Office of Disability Services. The Office of Disability Services at Rutgers, The State University of New Jersey, provides student-centered and student-inclusive programming in compliance with the Americans with Disabilities Act of 1990, the Americans with Disabilities Act Amendments of 2008, Section 504 of the Rehabilitation Act of 1973, Section 508 of the Rehabilitation Act of 1998, and the New Jersey Law Against Discrimination. https://ods.rutgers.edu

If you are a military *veteran* or are on active military duty, you can obtain support through the Office of Veteran and Military Programs and Services. http://veterans.rutgers.edu/

If you are in need of *mental health* services, please use our readily available services.
Rutgers University-Newark Counseling Center: http://counseling.newark.rutgers.edu/

If you are in need of *physical health* services, please use our readily available services.
Rutgers Health Services – Newark: http://health.newark.rutgers.edu/

If you are in need of *legal* services, please use our readily available services: http://rusls.rutgers.edu/

If you are in need of additional *academic assistance*, please use our readily available services.
Rutgers University-Newark Learning Center: http://www.ncas.rutgers.edu/rlc
Rutgers University-Newark Writing Center: http://www.ncas.rutgers.edu/writingcenter