Data Privacy (22:198:645:01)
Dr. Jaideep Vaidya (jsvaidya@business.rutgers.edu, x1441)
M 1:00-3:50 PM, 1WP-502

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 95/47, 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.

Prerequisites:

Undergraduate level knowledge in basic statistics and databases is needed.

Grading:

- Midterm Exam: 25%
- Final Exam: 30%
- Assignments and Class Project: 35%
- Class Participation: 10%

Class Project: Your project should 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.
I will put up a tentative list of project topics soon. You can choose from these, or identify your own.

Class Participation: 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.
**Final Exam:** The final exam will cover all of the material taught in the semester. It will test your understanding of the concepts learned throughout the semester.

**Exams:** There will be no make-up exams. You are required to present a written proof for situations such as going on to an emergency room due to unexpected and serious illness. Chatting during the exam is not allowed. Email communication during the exam will be considered cheating. No collaboration between class members will be allowed during any exam. There will be no extra-credit project.

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.

**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.

**Disability Statement:** Any student with a documented disability needing academic adjustments is requested to notify the instructor as early in the semester as possible, and must do so before the middle of the term. All discussions will remain confidential.

**Academic Integrity Statement:** Here at Rutgers Business School, our goal is to ensure that our students have a solid foundation that is grounded in integrity and respect of basic ethical principles. Rutgers University, in conjunction with the RBS Committee, has established an Honor Code that states:

“I pledge, on my honor, that I have neither received nor given any unauthorized assistance on this examination (assignment).” ([http://academicintegrity.rutgers.edu/integrity.shtml](http://academicintegrity.rutgers.edu/integrity.shtml))

In the future, students may be required to write and sign the Honor Pledge on every major paper, examination and assignment. This Honor Pledge will not displace, modify or amend the standards and procedures set forth in the Rutgers University Code of Student Conduct, ([http://judicialaffairs.rutgers.edu/university-code-of-student-conduct](http://judicialaffairs.rutgers.edu/university-code-of-student-conduct)), but simply suggest a higher set of standards to which RBS students adhere.

Students are encouraged to study together and to work together on class assignments and lab exercises; however, the provisions for Academic Honesty will be strictly enforced in this class. Every University student is responsible for upholding the provisions of the Student Code of Conduct. The policy on academic integrity can be found at [http://cat.rutgers.edu/integrity/policy.html](http://cat.rutgers.edu/integrity/policy.html). This is very important. Violations involving plagiarism and cheating, unauthorized access to University materials, misrepresentation/falsification of University records or academic work, malicious removal, retention, or destruction of library materials, malicious/intentional misuse of computer facilities
and/or services, and misuse of student identification cards will not be tolerated. Incidents of alleged academic misconduct will be handled through the established procedures of the University Judiciary Program. Refer to the policy for further details.

Frequently students will be provided with “take-home” exams or exercises. It is the student’s responsibility to ensure they fully understand to what extent they may collaborate or discuss content with other students. No exam work may be performed with the assistance of others or outside material unless specifically instructed as permissible. If an exam or assignment is designated “no outside assistance” this includes, but is not limited to, peers, books, publications, the Internet and the WWW. If a student is instructed to provide citations for sources, proper use of citation support is expected.

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 Outline:

Week 1  
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)  
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)  
We will discuss database privacy models, including the classic k-anonymity model, l-diversity, t-closeness, and differential privacy.

Week 4 (Statistical databases and query auditing)  
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 5 (Location privacy)  
We will look at the problem with privacy in mobile environments and location privacy issues.

Week 6  
Midterm Exam

Week 7 (Cryptographic essentials)  
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)  
We will look at the problems and techniques in privacy-preserving data mining.

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

Week 10 (RFID privacy)  
We will look at privacy issues in RFID devices.

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

Week 12 (Big data privacy)
We will look at the implications of big data on privacy.

Week 13
Project Presentations

Week 14
Final Exam

Reading List (to be updated):


List of relevant conferences and workshops

1. ACM Conference on Data and Application Security and Privacy (CODASPY) (http://www.codaspy.org/)
2. IFIP WG 11.3 Annual Conference on Data and Applications Security and Privacy (DBSec) (http://dbsec2014.sba-research.org)
4. Privacy Enhancing Technologies Symposium (PET) (http://petsymposium.org/2014/)
6. ACM CCS, IEEE S&P, ACM ASIACCS, etc..