PRIVACY, TECHNOLOGY, POLICY, AND LAW

GEORGIA INSTITUTE OF TECHNOLOGY
Fall 2016

CS 4726A, CS6726A, MGT 4726A, MGT 6726A, MGT 6726EM,
PUBP 4803PS, PUBP 8803PS

OVERVIEW OF THE COURSE

Course Purpose
There is a great need for qualified privacy professionals in industry and government. One need look no further than the number of data breaches facing industry and government institutions. The privacy field is maturing as evidenced by the fact that thousands of privacy professionals have been certified by the **International Association of Privacy Professionals**. This certification requires an understanding of technology, law and policy; this course exposes students to the complex interplay of these areas. This course will guide students in acquiring the skills needed to effectively design privacy into software while integrating with business practices across an enterprise in various contexts. It will provide an introduction to privacy policy and legal topics suitable for business, computing and public policy students. There is a great need for students to have a course that enables them to acquire the practical hands-on skills needed to be a successful privacy professional while also acquiring the basic grounding needed for more advanced research in areas such as software engineering. This course is expected to increase the practical and research skills of students specializing in business, computing, international affairs, and public policy.

Course Description
This mixed undergraduate- and graduate-level course takes a multi-disciplinary approach to the study of privacy—a current topic of great international interest for those in technology, policy, law, and/or business. The course is primarily lecture-based, with Socratic discussion of assigned readings, as well as active student participation via lively discussions and debates. Class sessions often include small-group, in-class activities to ensure hands-on experience in applying the concepts presented during lectures. There are no pre-requisites for this course, and students from varied backgrounds are welcome in the course.

Course topics include privacy engineering, big data, analytics, privacy policies, regulatory compliance, social networks, Internet of Things, behavioral advertising, ubiquitous computing, surveillance, wiretapping, and encryption. The course features group projects that engage students in real-world privacy challenges; specifically, compliance with new privacy regulations, development of an organization's privacy and security policies, and development of new privacy-sensitive approaches and/or tools for Internet technologies. The professors draw on their extensive experience in business, government, technology, and law to address current privacy debates.

Objectives
This course will enable students to understand how privacy is defined, protected, and managed in the areas of technology, business, policy, and law. Specific objectives include:

1. Examining the state-of-the-art for research and practice in information privacy, including methods, tools, notations and processes used in information systems;

2. Understanding the legal and policy issues surrounding technologies that operate on sensitive information;

3. Developing the multidisciplinary skills needed to analyze, manage, and resolve the challenges associated with privacy, technology, law, and policy;

4. Gaining a basic grounding for future technical research in privacy via the examination of current research issues and problems;

5. Gaining experience in handling real-world privacy challenges through analysis of software and business artifacts using written and oral communication; and

6. Learning how to write privacy and security policies for software systems and companies.

BASIC INFORMATION

Instructors:

Professor Annie I. Antón
School of Interactive Computing
Office: TSRB #211B
Phone: 404.894.8591
Email: aa16@gatech.edu
Office Hours: Tuesday 1:00–3:00 PM
or by appointment

Professor Peter Swire
Scheller College of Business
Office: Scheller #4163
Phone: 240.994.4142
Email: peter.swire@scheller.gatech.edu
Office Hours: Wed. 11:00 AM-12:00 PM
or by appointment

Teaching Assistants:

Marie Le Pichon
School of Interactive Computing
Phone: 713.826.6848
Email: marielepichon@gatech.edu
Office Hours: TBA

Swarnika Prakash
School of Interactive Computing
Phone:
Email: swarnika.prakash@gatech.edu
Office Hours: TBA

Class Time: Mondays 6:05 – 8:55 PM

Location: Scheller College of Business #200

Office Hours: We strongly encourage students to make at least one visit during either instructor's office hours over the course of the semester.

Course Website: All course materials are available via T-Square.

Class Text: All required material for this course will be available online through T-Square. Currently, no textbook exists for this course, but there will be an extensive amount of required reading in the form of academic papers and other readings related to privacy, security, law, and technology.

Course Resources: All reading materials and lectures are available in the <Resources> tab on T-Square.

Prerequisites: There are no prerequisites, and the multi-disciplinary nature of the material means that students from many backgrounds can benefit from the course. Open to both undergraduate and graduate students, with somewhat greater assignments for graduate students.

COURSE REQUIREMENTS AND GRADING

Weekly assignments are posted on the class website. Projects this fall will focus on a variety of privacy-related issues. We expect to have multi-disciplinary teams for the third assignment (including business, computing, and public policy) and for the final presentations. Grading is based on in-class participation, projects and class assignments. There are no examinations.

Reviews / Weekly Essays

All students are expected to complete the weekly reading assignments before the class in which they are discussed. The professors will post weekly questions based on the assigned readings. Undergraduates will write an answer (100 - 200 words in length) to one of the questions per week. Graduate students will write an answer for two questions each week (100 - 200 words in length for each question). Essays over 200 words will receive a one-point deduction.

Each weekly assignment is due by 10:00 AM the day it is scheduled to be discussed in class (Mondays at 10:00 AM). Weekly assignments should be submitted via T-Square with the filename "week02_firstInitialLastName". For example, the filename for the first assignment this semester (e.g. week02_aanton.docx). Please do not submit *.ps, *.pdf, *.doc or *.rtf attachment files).

Grading of Weekly Reading Essay

For each reading review question, grading will be: (1) zero points if not submitted; (2) one point if you submit a review but the quality is clearly low, such as not showing evidence that you have done the reading, or is outside the allowable word count in length; or (3) two points if the review shows evidence that you have done the reading and your comments are of reasonable quality. There are 12 classes with readings. For undergraduate students, the maximum point total is 24. A score of 20 or better will receive full credit - 15 points toward the final course grade. A score of 19 will receive 14 points, and so on. Your score goes down one point (such as from a 2 to a 1) if you submit it up to one week after the review is due. For graduate students, the maximum point total is 48. A score of 40 or better will receive full credit – 15 points toward the final course grade. A score of 38 will receive 14 points, and so on. There is no dropping of the lowest grade because it is built into the grading mechanism.

Projects

The class has the following project submissions: two essays to be submitted by each student individually and a three-part practical project to be completed in teams. The first two projects must conform to the *IEEE Transactions* Journal Paper template (available in the Project Resources folder on T-Square. A template example will be provided for the third project later in the semester.

Project Submission #1: Amendment to Rule 41 Essay

An update to Rule 41 of the Federal Rules of Criminal Procedure (Search and Seizure) will go into effect on December 1, 2016 if Congress does not take action otherwise.

Part 1:
In Part 1 of your essay you are an employee of the Federal Bureau of Investigation asked to write an essay explaining why the amendment should go into effect. Your superiors want you to explain why the amendment should be approved exactly as it is written, specifically addressing privacy concerns expressed by critics of the amendment. Your goal in this part of the essay is to persuade an undecided member of Congress to let the amendment go into effect on December 1 without further modification.

Part 2:
You are now an employee of the Privacy Rights Clearinghouse, which opposes the passing of this amendment. Giving particular attention to the long- and short-term privacy implications of the amendment, the goal in this part of your essay is to persuade an undecided member of Congress to take action to prevent this amendment from going into effect.

Part 3:
You are now a legislative assistant to a Senator who is undecided on the amendment. The Senator wishes you to explain your own view on whether to support or oppose this amendment.

All students are expected to have a bibliography for their essay, with proper citations. The bibliography does not count toward the assigned word limits.

Undergraduate students - 1,200 - 1,800 words in length
Grad students - 1,800 - 2,700 words in length

Essays must use the *IEEE Transactions* Journal Paper template (available in the Project Resources folder on T-Square), and must be submitted in .docx format.

Project Submission #2: Presidential Commission Recommendation
You have been selected to be on the team of Commissioners tasked with drafting a report for the White House on Enhancing National Cybersecurity. The goal of the report is "to enhance cybersecurity awareness and protections at all levels of government, business, and society, to protect privacy, to ensure public safety and economic and national security, and to empower Americans to take better control of their digital security." You have been asked to make one recommendation addressing this goal. Your recommendation should address both cybersecurity and privacy. Avoid cataloguing problems or simply addressing the symptoms and instead attempt to address the underlying issues our nation faces while grappling with the rapid pace at which technology is evolving.

Examples of topics include:

- *Information sharing* - The same information that might give clues about a cyber attack may also reveal personal information of non-attackers.
- *Mandated backdoors vs. encryption* - Mandated backdoors might provide clues about attackers but also provide access to personal communication.
- *Internet of Things* (smarthomes etc.) - If IoT security is badly done, then attackers can learn about the private space in peoples' homes. If security solutions require monitoring

of the home system, then the security system itself can perform surveillance.

- *Identity Management* (Identity proofing, federated identity) - Authentication classically involves who you are, what you have, or what you know; the authentication databases that store this information can be a path to compromising personal secrets and biometrics.
- *Government access to data* - As the Microsoft Ireland example shows, many cyber attacks cross borders; how can we provide needed insights to the defenders in more than one nation without also creating leaks that go to the attackers?
- *Surveillance of employees* - To improve security, the organization may wish to conduct comprehensive surveillance and background checks but that may intrude on employee privacy and create databases about the employees that are subject to breach.

If you are not sure whether your topic addresses cybersecurity or has strong enough privacy implications, we encourage you to come to Marie or Dr. Antón's office hours.

Requirements:

- Explain how it improves both cybersecurity and privacy
- Structure each recommendation in three parts:
    - Current state;
    - Why change is needed; and
    - Actionable near- and long-term recommendations and why they would be better than what we have now.
- All students are expected to have a bibliography for their essay, with proper citations. The bibliography does not count toward the assigned word limits.
- **Undergraduate students** - 1,200 - 1,800 words in length
- **Grad students** - 1,800 - 2,700 words in length
- Essays must use the *IEEE Transactions* Journal Paper template (available in the Project Resources folder on T-Square), and must be submitted in .docx format.

Project Submission #3: Privacy and Security Policy

For this group project submission, your team will draft a Privacy and a Security policy for your company's commercial drone service. You must comply with any and all regulations pertaining to privacy that govern the use of your drone service. It is up to you to decide to what extent you will follow guidance issued by different private and public sector entities regarding privacy concerns and drones. The Privacy and Security policies must be consistent with each other as graders will be looking for potential conflicts between the two documents.

You will also write a short memorandum to your parent company's Board of Directors (no longer than 750 words) for their quarterly meeting explaining the Privacy and Security policies and justifying the content, including how the Privacy and Security policies comply with applicable regulations and to what extent you have decided to (or not to) follow other relevant industry standards and best practices. Assume that the drone operations are a subsidiary of a large public company and that the reputation of the company will be affected by the decisions you make in your privacy and security policies.

PSA Presentations
During finals week, in place of an examination, each project team will present a Public Service Announcement video aimed at increasing public awareness of privacy and/or cybersecurity. The video should be 30-90 seconds long. Unless there's an objection from a team member, the best videos will be made available to share outside of the classroom via the WWW and/or a privacy organization.

The video *for each presentation should be submitted via T-Square with the filename "[teamN_psa]" by noon on the day before the scheduled presentation.*

Class Participation
Attendance is required. Students will participate in class discussions. This will be done via an "on call" group assignment established by week 3 of the semester. Students will be assigned to one of *n* different "on call" groups.

Attendance will be monitored via a sign-in sheet for each class. There are 14 class sessions in addition to the final exam period. **You may miss up to one class session without an excuse. Any unexcused absence beyond the first, will result in a 5-point deduction in your final grade.** Excused absences must be explained in writing (email is permitted), and can be for the following reasons: (1) illness; (2) death or illness in the family; (3) jury duty; (4) military obligation; (5) documented obligations to attend Institute sponsored events (such as described in a GTAA travel letter); or (6) religious holiday. Additional reasons may be excused only with permission of the instructor.

Students arriving 10 or more minutes after the start of a class, or leaving before the end of a class, will be considered absent (unexcused) for that class (regardless of whether the student was present when attendance was taken) unless the student receives permission from the instructor to arrive late or leave early.

Students are expected to sign the attendance sheet by the door at the beginning of each class session.

Students must be thoroughly prepared to actively discuss in class on the "on call" days to which they are assigned. Preparation may include formulating and bringing discussion questions and reading supporting material to address weaknesses or concerns raised by assigned readings. If for any reason, a student is unable to be prepared for class on any given day, they must let the instructor know **before** class begins. *Students are able to take a "pass" during one class session for which they were on call over the course of the semester.*

Evaluation Procedures
Final grades in the course will be determined as follows:

Weekly Essays	15%
Class Participation **	15%
Amendment to Rule 41 Essay	15%
Presidential Commission Recommendation	20%
Privacy and Security Policy	25%
Public Service Announcement	10%

**Note: class attendance is required.

The grading scale for your final grade will be as follows:

A	90 ≤ Final Grade ≤ 100
B	80 ≤ Final Grade < 90
C	70 ≤ Final Grade < 80
D	60 ≤ Final Grade < 70
F	Final Grade < 60

Grading Breakdown
The syllabus lists the papers scheduled over the course of the semester that students must review. Overall, weekly essays are worth 15% of your final grade.

Class participation is also worth 15% of your final grade. Course attendance is necessary, but not sufficient. **Students must be well prepared during their on-call weeks and actively ask questions in class to earn credit in this area.**

Course Projects
All projects shall be submitted via T-Square. There are three course projects and one project presentation that students must complete. They are due on the following dates and worth the following percentages:

Amendment to Rule 41 Essay (15%)	Due: 9/15/2016 at 6:00 PM
Presidential Commission Recommendation (20%)	Due: 10/19/2016 at 6:00 PM
Privacy and Security Policy(25%)	Due: 12/1/2016 at 6:00 PM
Final PSA Video (10%)	Due: 12/12/2016 at 10:00 AM

Additional Important Dates for In-Class Activities:

Project #1 Q&A	8/29/2016
Team Assessment Surveys	9/26/2016
Project #2 Q&A	9/26/2016
Team Assignments and Group Meetings	10/3/2016
PSA Q&A	10/3/2016
PSA Concept Discussions	10/17/2016
Project #3 Q&A	10/24/2016
PSA Storyboard Discussions	11/7/2016

• *Extensions are available on an individual basis with prior approval by the instructor.*

COURSE CALENDAR & CONTENT

Week 1 (Aug. 22): Introduction to Privacy, Technology, Policy, and Law
Week 2: (Aug. 29): Fourth Amendment and Technology
Week 3: (Sept. 5) *Labor Day*
Week 4: (Sept. 12) Foreign Intelligence, Surveillance, and Privacy
Week 5: (Sept. 19) Defining Privacy
Week 6: (Sept. 26) Cybersecurity Commission
Week 7: (Oct. 3) Regulatory Compliance & GLBA / HIPAA & Guest Speaker
Week 8: (Oct. 10) *Fall Break*
Week 9: (Oct. 17) Social Networks
Week 10: (Oct. 24) Privacy Engineering and Privacy Policies
Week 11: (Oct. 31) Big Data and Analytics
Week 12: (Nov. 7) Anonymity and Reidentification
Week 13: (Nov. 14) Differential Privacy and Discriminatory Algorithms
Week 14: (Nov. 21) Behavioral Advertising & Tracking Technologies
Week 15: (Nov. 28) The Potential Privacy Crisis with Europe
Week 16: (Dec. 5) Encryption
Finals Week: (Dec. 12) Project Presentations

COURSE EXPECTATIONS & GUIDELINES

Late Policy
Each weekly assignment / essay is due by 10:00 am the day it is scheduled to be discussed in class (Monday morning). Late reviews will be docked one letter grade for up to one week after the day it is due, and will not be accepted after that. Paper reviews should be submitted via T- Square.

Each project deliverable is due as specified in the calendar and in the syllabus above. Late project deliverables will be docked one letter grade per day of the week. Thus, if a project deliverable is due on Monday, but submitted on Tuesday, the highest grade possible on that deliverable is a B, etc.

Academic Integrity
The course will follow all relevant and appropriate Georgia Institute of Technology academic regulations (**http://www.honor.gatech.edu**) including those about academic integrity. All students are expected to maintain traditional standards of academic integrity by giving proper credit for all work. Webster's defines plagiarism as "to steal and pass off (the ideas or words of another) as one's own: use (another's production) without crediting the source." A student shall be guilty of a violation of academic integrity if he or she represents the work of others as his or her own or aids another's misrepresentation. All suspected cases of academic dishonesty will be aggressively pursued according to the Georgia Tech Academic Honor Code. **Any violation associated with a homework, assignment, project, examination or quiz will result in a zero for the assignment and a failing grade for the course.** Such violations will be reported to the Office of Student Integrity (OSI), which may impose penalties beyond those by the instructor(s).

In this course, each student is expected to work independently on the first writing assignment;

not working independently on the first assignment will be considered a violation of the GT Academic Honor Code. Submitting any work other than your own, including a sentence without proper quotation marks with citation to the original source, is also a violation of the student honor code.
For any questions involving these or any other Academic Honor Code issues, please consult the professor(s) or www.honor.gatech.edu." Students are also encouraged to read the ACM Code of Ethics (**http://www.acm.org /constitution/code.html**), particularly sections 1.3, 1.5, 1.6, 2.2 and 2.4.

Accommodations for Students with Disabilities
The course process will follow all relevant and appropriate Georgia Institute of Technology academic regulations including those relevant to students with disabilities. Any students requiring additional assistance due to disabilities (e.g., learning disabilities) should contact the professor(s) during the first week of the semester. Students requiring extra time for examinations and quizzes are asked to make arrangements at least three days in advance. You may contact the ADAPTS (**http://www.adapts.gatech.edu**) regarding campus services.

Discrimination and Harassment
Georgia Tech does not discriminate against individuals on the basis of race, color, religion, sex, national origin, age, disability, sexual orientation, or veteran status in the administration of admissions policies, educational policies, employment policies, or any other Institute-governed programs and activities. This class adheres to those guidelines. Alternative viewpoints are welcome in this classroom. However, statements that are deemed racist, sexist, classist, or otherwise discriminatory toward others in the class will not be tolerated.

No form of harassment or discrimination is allowed in this class. In keeping with the professional nature of this course, only professional behavior is acceptable between the instructor and the students and between students. No harassment of any kind is allowed in class including but not limited to gender, age, ability, religion, sexual orientation, and ethnicity.

MISCELLANEOUS

Legal Disclaimer
Any and all opinions or statements made by the instructors are for classroom purposes only and are not intended and should not be construed as dispensing legal advice or creating an attorney-client relationship. This disclaimer includes conversations with students during and outside of class. The instructors are not permitted to provide personal legal advice to students. Under no circumstances will an attorney-client relationship exist between the instructor and a student.