This course would be offered as a second or third-year level, two-credit (Grading Option A) course. The course may be offered for the first time during the Fall 2015 semester.

Although not a requirement, eligible students ideally will have already taken and passed:

- U.S. Constitutional Law
- Torts II

COURSE DESCRIPTION

This course will provide the students with an introduction to data privacy law and the use of personally identifiable information ("PII"). The primary purpose of the course is to allow students to better understand how courts and legislatures protect information as new technologies and institutional practices emerge. This course will explore the roots of privacy law, its evolution in the 20th century, and the challenges of regulating information, both foreign and domestic, in the Digital Age. This exploration will occur by examining the U.S. Constitution, rules, regulations, and cases that apply to collecting, using, and disclosing personal information.

COURSE MATERIALS


Daniel J. Solove  
Professor of Law  
George Washington University  
Law School

Paul M. Schwartz  
Professor of Law  
U.C. Berkley School of Law

COURSE REQUIREMENTS

- Students must attend 90% of the schedule sections and receive a passing grade on the final exam in order to receive credit for this course. Attendance will be taken at every section through the use of a sign-in sheet.
• Students will be called on and must be prepared to discuss the reading material and examples during each section of class. Failure to be properly prepared for class without prior communication with the professor may result in a failing grade.

• Presentation. I am considering offering an opportunity to add extra points to their final exam score by completing a presentation on an emerging privacy issue raised by technology or some other use of personal information during section 4.

• Students will take a 2.0 hour, closed-book multiple choice and short essay exam.

**COURSE RATIONALE**

Privacy has become one of the defining topics of the Digital Age. This is because technology has made it easier to both obtain and maintain information about others. This information, which is collected by individuals, businesses, and the government, includes, among other things, medical records, financial transactions, social media posts and physical movements ("geo tracking"). With all this information now available, concerns have arisen about how it will be safeguarded and used. This in turn has led to the creation of new privacy-related laws, rules, and procedures both in the United States and abroad. Newly minted attorneys must be able to not only interpret and apply these laws, but also draft new legislation, policies and contracts to address future privacy concerns. This course will help prepare law students to meet these challenges.

To date, approximately 40-50 law schools offer courses on privacy law. Also, at least one law school (Univ. of Santa Clara) offers a certification and another school offers an LLM (John Marshall) in privacy law. There are also several law school text books on the topic.

**Careers in privacy for attorneys.**

When I started as a privacy officer in 2003, there were but a few thousand worldwide. Today, the profession has grown exponentially, with more than 20,000 members of the International Association of Privacy Professionals, alone. Law firms with committed privacy practices have likewise grown considerably since 2003. Government agencies also have committed privacy officers and departments committed to dealing with privacy related issues. Regardless of sector, however, attorneys have to have a foundational knowledge of information privacy to be effective and avoid common pitfalls not only for their clients, but for their own practices.

Almost every business in operation today deals with privacy, be it data about employees, customers, vendors, and others. They are developing new products and
services centered on the use of such personal information. Companies failing to comply with the myriad of laws will find themselves heavily fined, sued often, or simply put out of business. Regulatory action and related fines are on the increase. Breach notification laws also impose huge costs—not only in money but in opportunity costs. Time taken to deal with a data breach, is time not making widgets. And, of course, this is nothing to say of lawsuits—especially class action litigation pertaining to a duty of care with respect to PII.

**SESSION TOPICS/READING**

**Section 1: The Foundations of Privacy as Personal Value and Legal Construct, Privacy in the United States**


This section shall be an introduction to privacy law, in which we will discuss privacy as a personal value defined by the individual to the construction as a right or privilege under the law today. I will provide an introduction and overview of data privacy, specifically reviewing:

**Basic Privacy Principles and Concepts**

- Personally Identifiable Information
- Anonymity
- Identification
- De-Identification
- Expectation(s) of Privacy

**Privacy in the U.S.: The Citizen-Government relationship**

- Key Constitutional Law cases involving the First and Fourth Amendments
- National Security and Surveillance Law
- Privacy of Government Records
We shall then turn to a short review of the privacy torts (appropriation, intrusion, false light and disclosure of private facts) using some case law. We will then conduct a broader, in depth discussion on the challenges of existing state laws and their impact on individual rights, commercial rights and government rights.

Topics will include:

- Medical and Genetic Privacy
- Financial Privacy
- Privacy and the Media

Section 2: Privacy Outside the United States

Related Text: Solove, selections from pgs. 995-1071

In this section, we will have a discussion on the existing privacy frameworks in other countries and regions to include:

- European Union
- Canada
- South America
- Asia-Pacific Region (APEC)
- OECD Guidelines

Class discussion will compare and contrast the U.S. framework with those in other countries, as well as exploring the fundamental differences between privacy as a basic human right and that of a privilege under law.

Section 3: Privacy in the Digital Age and Consumer Privacy

Related Text: TBD (Professor-provided materials, TWEN material, and articles from recent publications)

In this session we will discuss and review the relevant technologies shaping privacy law today to include:

- Consumer tracking and marketing
- Location-based tracking
- RFID
- Facial recognition software
- Wearable technology
- Data linking
We will discuss the challenges the Internet presents to both privacy and the enforcement of any laws and regulations in cyberspace. I may also invite a guest speaker to add value to this discussion to include demonstration of these technologies.

Section 4: Emerging Issues in Privacy

Related Text: *TBD*. (Professor-provided materials, TWEN material, and articles from recent publications)

In this section, we will explore emerging issues and current events implicating privacy and potentially complete a class exercise in assessing the policy and legal implications of a new technology or proposed use of personal information.

Students may have an opportunity to pick and present on an emerging issue.

Session Five: Practical Privacy Best Practices for You and Your Clients

Related Text: *TBD*. (Professor-provided materials, TWEN material, and articles from recent publications)

In line with our school mission of creating lawyers who are problem solvers and our reputation of providing practical skills to enable them to hit the ground running, I will conduct a discussion on the basic components law clients need to have in a responsible information management program.

- Data Categorization and Mapping
- Privacy Policy and Procedures
- Online Privacy Notices
- Drafting data protection agreements
- Data security best practice
- Data breach response management

I will provide the students with the practical tools they can use in assisting their clients and/or setting up their own business.