The Intersection of Terrorism & Privacy Rights
FALL 2016

Day/Time: MW 5:45-7:10
Location: ES0139
Instructor: James R. Clark, Esq.
Contact: 518-368-8774/jrclark@suny.edu

Office Location and Hours: Humanities B-16, MW 7:15-8:15PM

Course Information:

Course Description:
This survey course will introduce students to “privacy law” and how it applies to government counter-terrorism activities and disaster response in a post 911 world. Students will trace the historical and foundational privacy law principles in both the public and private sectors and the dynamic factors that influence it. Students will also explore the balance between the needs of law enforcement in conducting counter-terrorism operations and individual civil liberties in fighting the war on terror. Through the use of select readings and important court decisions, students will be introduced to the concepts of individual expectations of privacy and confidentiality and how those concepts relate to various legal frameworks in fighting terrorism. Students will look at information privacy issues in the context of new technologies, security risks and institutional practices and the philosophical principles that shape privacy law.

Course Structure and Requirements:
This course will be taught in a seminar style format utilizing the Socratic method of teaching. Students will be encouraged and expected to participate in class discussions focusing on the material assigned for each class. Students will also be expected to make cogent arguments based upon the material assigned from opposing viewpoints. Grading consists of periodic in class assignments/quizzes, two exams (mid-term and final) and points given for class participation (see “Grading” below).
Text and Materials

- **Instructor Provided Materials:** Reading materials (.pdfs), videos, etc., will be made available to students via Blackboard and will generally follow the readings listed in the syllabus. While I anticipate the readings and materials will follow the those outlined in the syllabus, I reserve the right to change, modify, add to or subtract from, the readings and materials. However, the readings and materials you will be responsible for will be those available via Blackboard. *(PLEASE NOTE: Reading assignments may be limited within each document – discussed later in syllabus).*

Course Learning Objectives:

Upon completion of this course, students should be able to:

1. Demonstrate an understanding of the history privacy law and factors impacting it;
2. Summarize how privacy laws are developed and factors that influence its development;
3. Understand, identify and compare the methodologies used by counter-terrorism forces in fighting terrorism and how those methodologies intersect with individual privacy;
4. Identify and analyze key arguments supporting strong individual privacy law protections and those supporting aggressive counter-terrorism tactics;
5. Articulate differing viewpoints based upon applying key *Fourth Amendment* principles to a given fact pattern.
6. Analyze facts of a given situation and explain how they relate to informational privacy and counter-terrorism;

Prerequisites:

*There are no prerequisites for this course.*

Grading:

This course is A-E graded and the grades are determined based on the following criteria:

Each student will have the opportunity to earn up to 1000 points through a combination of class assignments, class participation, quizzes, and two exams (mid-term and final).

Exams:

Mid-Term is worth 300 points. *(Structured Case Study: 6-8 pages, including title page, sources cited page).*

The Final is worth 400 points.
Class Assignments/Quizzes/Participation are worth 300 points.

**Grading Scale (based on 1000 total points)**

<table>
<thead>
<tr>
<th>Grade</th>
<th>Points Range</th>
<th>Grade</th>
<th>Points Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>950-1000</td>
<td>C</td>
<td>730-760</td>
</tr>
<tr>
<td>A-</td>
<td>900-940</td>
<td>C-</td>
<td>700-720</td>
</tr>
<tr>
<td>B+</td>
<td>870-890</td>
<td>D+</td>
<td>670-690</td>
</tr>
<tr>
<td>B</td>
<td>830-860</td>
<td>D</td>
<td>630-660</td>
</tr>
<tr>
<td>B-</td>
<td>800-820</td>
<td>D-</td>
<td>600-620</td>
</tr>
<tr>
<td>C+</td>
<td>770-790</td>
<td>E</td>
<td>0-590</td>
</tr>
</tbody>
</table>

**Expected Class Preparation and Reading Efforts:**

This course will guide the student through the broad study of Privacy Law and its specific application to counter-terrorism efforts. All readings and materials will be provided by the Instructor and will be used to provide an important analysis of the fundamental principles relating to privacy law. I expect you to carefully read or view the assignments posted via Blackboard prior to each class as they will be instrumental to our discussions and class assignments/quizzes. I will periodically provide you with guidance as to which “sections” of the documents on which your studies should focus. In most cases, I am looking for you to gain an appreciation and understanding of the major elements of the reading. The class assignments/quizzes will not require extremely detailed recall on your part but rather your recollection and understanding of the major elements (discussion or reading assignments) of the previous class.

**CLASS 1**

**INTRODUCTIONS AND WELCOME**

The first class will be dedicated to class introductions and a general discussion of what privacy means to you and the class' collective understanding of terrorism. Students are expected to have completed the readings for Class 1 prior to attending class.

**Reading**

- Brandeis and Warren, “The Right to Privacy” (1890)

**CLASS 2**

**THE SCOPE OF INFORMATION COLLECTION**

In Class 2, students will look at the universe of information that can be collected and potentially protected by privacy laws and policies, including how such information is collected, stored, shared, and maintained.

**Reading**
CLASS 3

DEFINING PRIVACY AND TERRORISM

In Class 3, we will explore the legal definitions of privacy and terrorism and begin to explore the historical breadth of privacy law and its sources.

Reading

- 18 U.S.C. §2332b
- Acts of Terrorism Transcending National Boundaries
- 22 U.S.C. §2656f
- Annual Country Reports on Terrorism (US Dept. of State)
- Olmstead v. United States 277 US 438 (1928)

CLASS 4

HISTORY AND SOURCES OF PRIVACY LAW

In Class 4, we continue to look at the fundamentals of privacy law and its historical origins, types and perspectives, including: Constitutional law; Common Law; and Statutory Law.

Reading

- Informational Privacy Law (Solove & Rotenberg), pgs 18-31
- Informational Privacy Law 5th Edition, (Solve & Swartz, 2015), pages 1-3 (Introduction to Privacy)

CLASS 5

PRIVACY TORTS

In Class 5, we look at the civil law of privacy by directing our discussion to privacy torts and how they apply in particular situations and looking at specific court cases.

Reading
• Prosser’s Privacy Law: A Mixed Legacy (Daniel J. Solove)
• Neil M. Richards, The Limits of Tort Privacy, 9 J. on Telecomm. & High Tech. L. 357, 378 (2011)
• Right to be forgotten: Google Spain, S.L. Google Inc. y Agencia Espanola de Proteccion de Datos (AEPD) European Court of Justice, EU:C:2014:317 [pgs 1152]
• ACLU v Miller, 977 F.Supp. 1228 (N.D. Ga. 1997)
• Lake v. Wal-Mart, 582 N.W.2d 231 (Minn. 1998)

CLASS 6

FOIA/FOIL AND PERSONAL PRIVACY PROTECTION LAWS

In Class 6, students will look at government statutory authority to collection personal information and public access to personal information under federal and New York State law.

Reading

• Informational Privacy Law (Solove & Rotenberg, Aspen Publishing), pgs 445-475 (FOIA And Privacy Act of 1974)
• NYS Department of State, Committee on Open Government (Public Officers Law, Article 6, sections 84-90 - Freedom of Information Law)
• NYS Department of State, Committee on Open Government (Public Officers Law, Article 6-A, sections 91-99 - Personal Privacy Protection Law)

CLASS 7

THE 4TH AMENDMENT AND PRIVACY

Class 7 begins our study of the 4th Amendment and its application to informational privacy in the terrorism context.

• What is it?
• How does it work?
• When is it applied?

Reading

• 4th Amendment
• Informational Privacy Law 5th Edition, (Solve & Swartz, 2015), pages 258-267, 288-301
CLASS 8

In Class 8, we continue our study of the 4th Amendment by looking at electronic surveillance by the government and the privacy interests at stake.

ELECTRONIC SURVEILLANCE - PART 1

- Electronic Communications Privacy Act (Title I, Title II, and Title III)
  - Aural Communications
  - Oral Communications
  - Electronic Communications
- The Wiretap Act (Title I)
- The Stored Communications Act (Title II)

Reading

- EPIC - Electronic Communications Privacy Act (ECPA)
- Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004)
- United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)
- Microsoft v. United States (July 2016)

CLASS 9

ELECTRONIC SURVEILLANCE - PART 2

In Class 9, we continue our look privacy and government electronic surveillance.

- Pen Register Act (Title III)
- Communications Assistance For Law Enforcement Act
- Foreign Governments

Reading

- U.S. Weighs Wide Overhaul of Wiretap Laws
- Law Enforcement Cross-Border Data System: DOJ Legislative Proposal
- Law Enforcement Cross-Border Data System Needs Fix _ DOJ _ Bloomberg BNA.pdf

CLASS 10

In Class 10, we turn our attention to digital searches conducted by the government and how such searches impact individual privacy interests in personal electronic devices, such as computers and smartphones.
• Computer and Cellphone Data Searches
• Email
• Encryption
• ISP information
• All Writs Act, 28 USC 1651

Reading


CLASS 11

In Class 11, we turn our attention to the part of the 4th Amendment involving the element of video surveillance and tracking by government and how the principles of the 4th Amendment may apply in counter-terrorism investigations.

GROUND BASED VIDEO SURVEILLANCE – PART 1

• Ground Based Camera Systems
• Dash Cameras
• Body Cameras

Reading

• Informational Privacy Law 5th Edition, (Solve & Swartz, 2015), page 383
• Oliver v United States (Open fields)
• Rutledge, Devallis “Legal Issues With Body Cameras”
• Police – The law Enforcement Magazine January 26, 2015
• The Daily Gazette Article Series
• Informational Privacy Law 5th Edition, (Solve & Swartz, 2015), page 383
• United States v. Vargas

CLASS 12

GROUND BASED VIDEO SURVEILLANCE & MORE– PART 2

• GPS Tracking
• Cellphone Tracking (Stingray)
• Thermal Imaging
• LPRS

Reading

• Can You Hear Me Now? How Police Track Your Cellphone
• Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators
• Lopez v US (Observations)
• United States v. Jones (GPS Tracking)
• Kyllo v. United States (Thermal imaging)
• United States v. Lambis, July 12, 2016 (Cellphone Tracking)
• State v. Andrews (March 2016)

CLASS 13

In Class 13, we look at Ariel based surveillance and privacy issues.

ARIEL BASED VIDEO SURVEILLANCE

• Unmanned Aircraft Systems (UAS)

Reading

• Observations from Above: Unmanned Aircraft Systems and Privacy, pages 458-498
• Presidential Memorandum (Safe Guarding Privacy)
• Unmanned Aircraft Systems: Key Considerations Regarding Safety, Innovation, Economic Impact, and Privacy
• SOFREP News 6/21/2016
• Theintercept June 21, 2016

CLASS 14 – Mid-Term- CLASS TBD

CLASS 15

WHAT ABOUT THE 1st AMENDMENT, PRIVACY AND TERRORISM?

In Class 15, we look at the how the First Amendment relates to individual privacy and counter-terrorism.

Reading

• 1st Amendment
• Terrorism and the First Amendment
• Why Tolerate Terrorist Publications?
• United States v. Mehanna
• SCOTUSblog: Challenging use of advocacy as terrorism
• American Freedom Law Center - Terrorism Advertisement
CLASS 16

GOVERNMENT INFORMATION COLLECTION AND THE WAR ON TERROR – PART 1 – September 11th and Terrorism

In Class 16, we begin a series of classes that look closer at government surveillance in the context of collecting personally identifiable information (PII), information sharing and the government privacy policies behind information gathering. We start with the need for intelligence gathering, the communities that gather intelligence, and how law enforcement’s approach has changed since 9/11.

- September 11th, 2001
- The Intelligence Community
- Government and Law Enforcement Reaction

Reading

- The Impact of Terrorism on State Law Enforcement, Adjusting to New Roles and Changing Conditions
- Intelligence and Its Role in Protecting Against Terrorism

CLASS 17

GOVERNMENT INFORMATION COLLECTION AND THE WAR ON TERROR – PART 2 – Is Data Mining the Answer?

- FUSION Centers
- Government Data Mining and Associated Privacy Risks
- Federal Agency Data Mining Reporting Act of 2007
- Collection, Use, Storage, Dissemination, Destruction

Reading

- Intelligence Fusion Center: A Decentralized National Intelligence Agency
- Study: Violations of Privacy Rights By Fusions Centers
- 42 U.S. Code § 2000ee–3 - Federal agency data mining reporting
- Privacy Risks Presented By Government Data Mining
- Data Mining, Dog Sniffs, and the Fourth Amendment

CLASS 18

NATIONAL SECURITY & PRIVACY POLICY
The next series of classes drill down into National Security and Foreign Intelligence and legal framework surrounding government information collection in the national security realm and the related privacy implications.

- Government Intelligence Communities
- Foreign Intelligence Surveillance Act (FISA)
- Snowden Revelations

Reading

- *Executive Order 12333*
- *Balancing Intelligence Gathering and Privacy*
- *Snowden Revelations Led to 'Chilling Effect' on Pursuit of Knowledge: Study*

CLASS 19

GOVERNMENT SURVEILLANCE PROGRAMS, SYSTEMS AND INFORMATION COLLECTION

- National Security Administration (NSA) Surveillance
- The PATRIOT Act Revisited: §215 and §702
- USA Freedom Act

Reading

- *So What Does the USA Freedom Act Do Anyway?*
- *USA FREEDOM Act Reinstates Expired USA PATRIOT Act Provisions but Limits Bulk Collection*

CLASS 20

GOVERNMENT SURVEILLANCE PROGRAMS, SYSTEMS AND INFORMATION COLLECTION

- Total Information Awareness Program (TIA)
- PRISM and Upstream

Reading

- *Report of the Technology and Privacy Advisory Committee: Total Information Awareness Program*
- *United States v. Hasbajrami (March 2016)*
• Department of Homeland Security Privacy Office 2015 Data Mining Report to Congress February 20
• Privacy Impact Assessment for the Secure Flight Program (2007)
• Privacy Impact Assessment for the Automated Targeting System (2007)

CLASS 21

COUNTERTERRORISM, PRIVACY AND GOVERNMENT’S RESPONSE

Sectorial Protections and Government Policies

• Constitutional Protections Revisited
• Sectorial Protections
• Government Policies

Reading

• Informational Privacy and Its Protection from Intrusion by the Government
• Principles for Government Data Mining Preserving Civil Liberties in the Information Age, pages 1-19

CLASS 22

COUNTERTERRORISM, PRIVACY AND GOVERNMENT’S RESPONSE: HOW IT WORKS

• DHS Privacy Office
• Director of National Intelligence: Privacy Guidance

Reading

• DHS Privacy Office, Guide to Implementing Privacy
• Properly Obtaining and Using Publicly Available Information

CLASS 23

THE COLLECTION OF FINANCIAL INFORMATION IN FIGHTING TERRORISM

Readings

• The Right to Financial Privacy Act (EPIC)
• Combating Terrorist Financing in the United States: The Role of Financial Institutions (911 Commission)
• What Financial Institutions Should Know Before Answering That Subpoena
CLASS 24

THE COLLECTION OF HEALTH INFORMATION IN FIGHTING TERRORISM: HIPAA

In Class 24, we begin looking at HIPAA and personal health information in fighting terrorism.

- Legal Protection of Health Information
- Health Information and Cyberterrorism

Readings:

Law Enforcement & National Security Access to Medical Records (cdt.org)
Health Information: The New Terrorist Target
Fundamentals of Privacy Law, (Solove) – Chapter 6
From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine Part I: Conceptual, Moral and Legal Foundations; American College of Emergency Physicians
November 2014 Bulletin: HIPAA Privacy in Emergency Situations
Combating Terrorist Financing in the United States

CLASS 25

In Class 25, we begin looking at personal health information and its relationship with emergency management.

THE COLLECTION OF HEALTH INFORMATION IN FIGHTING TERRORISM: FUSION CENTERS & EMS

- HIPAA and the War on Terror - “Security Rule”
- Fusion Centers, Health Information and Emergency Medical Service Personnel

Readings

- National Network of Fusion Centers Fact Sheet (DHS.gov)
- Health Security: Public Health and Medical Integration for Fusion Centers (it.ojp.gov)
- Petrie, Michael. The Use of EMS Personnel as Intelligence Sensors

CLASS 26

SOCIAL MEDIA, TERRORISM PREVENTION AND PRIVACY RIGHTS

Readings
• Privacy, Public Safety Collide as Terror Groups Collaborate on Social Media (govtech.com)
• Obama: Monitoring Terrorists on Social Media Must Be Balanced with our Values (Britbart)
• Fighting Terrorism on Facebook Isn’t That Easy (morningconsult.com)

CLASS 27

WRAPPING IT UP AND PULLING IT ALL TOGETHER!

In Class 27 students will discuss the overall importance of privacy law as it applies to both government and the private sector. By review of what has been learned throughout the semester, students will be challenged to consider the future of counter-terrorism efforts and how privacy law principles may influence those efforts for better or worse and the stakeholders that will influence the potential outcomes.

Policies:

Attendance Policy: Students are expected to attend each class or provide a written excuse for why they could not attend. Absences may negatively impact your grade for class participation.

Disability Policy: Reasonable accommodations will be provided for students with documented physical, sensory, systemic, cognitive, learning and psychiatric disabilities. If you believe you have a disability requiring accommodation in this class, please notify the Director of the Disability Resource Center (Campus Center 137, 442-5490). That office will provide the course instructor with verification of your disability, and will recommend appropriate accommodations.

Academic Dishonesty Policy: Students are expected to comply with the University at Albany’s Community Rights and Responsibilities. An incident of unethical conduct (e.g. cheating, plagiarism) or classroom disruption will result in a Fail and referral to the appropriate Departmental and University Committees. More information on academic integrity is available at the following website: http://www.albany.edu/reading/academic_integrity.php. Students will be asked to sign a statement of honor, promising to act with academic integrity.

Electronic Devices:

Electronic devices (laptops, cell phones, etc.) are permitted in the classroom provided they are in silent mode and are not a distraction to the class as determined by the instructor. Use of laptops and cell phones for texting and voice calls is permitted outside of the classroom during class to avoid disrupting classroom presentations and discussions.