

SYLLABUS
GLOBAL COMPLIANCE IN THE DIGITAL AGE

Prof. Kenneth N. Rashbaum
krashbaum@bartonesq.com
212-885-8836 (office)
973-222-1988 (mobile)

Class Time: Tuesdays, 8:10 AM-10:00 AM

Class will not be held on October 21 and 28. Makeup classes will be scheduled.

Room: 243

Book and Additional Readings:

Text: Paul, George, *Foundations of Digital Evidence* (ABA Publishing, 2008) (hereafter “Paul”).

Links to additional readings will be distributed to students, and case citations will be provided for selected assignments. Documents assigned from The Sedona Conference® may be downloaded from the Conference website, www.thesedonaconference.org.

COURSE DESCRIPTION

Welcome to Global Compliance in the Digital Age. This course explores and analyzes the statutory and regulatory compliance challenges for management of electronic information for e-commerce and litigation discovery across industries and the barriers of national cultures, histories and differing legal systems.

To reach an understanding of the compliance network for electronic information, we will analyze how differing notions of “personal information” in privacy and data protection laws and regulations impact the daily interfaces essential to e-commerce. The structure of common law and civil law systems will be compared with regard to standards of disclosure of electronic information for litigation and arbitration. We will examine practical frameworks for management of data in healthcare, finance, education and other regulated areas. U.S. federal and state information compliance schemes will be analyzed. The practical impacts of these laws and regulations on the daily activities of corporations and individuals and business and litigation will be seen in drafting exercises that will include preparation of discovery requests and responses; internal memoranda; information governance policies and procedures; and training materials.

We will explore and analyze legal and regulatory complexities in social media, and practical aspects of information governance, including cloud computing and privacy. Does it exist, when Google, for example, has stated in federal court that employees or Google algorithms read every Gmail, Terms of Use of most social media sites permit the provider to use any information uploaded to the service in almost any manner it sees fit, and the National Security Agency (NSA) can bypass most encryption methods?..

The class will also comprise an overview of privacy and data protection provisions in Europe, Asia and South America and, as a **Learning Objective**, you will understand and be able to apply the following concepts: how U.S. courts have approached the dilemma of conflicts with privacy and data protection laws of other nations, including relevant treaties; trends toward reconciliation of the blurred cyber-borders of international e-commerce with established political boundaries; and collection of electronic evidence from abroad with an eye toward admissibility requirements.

Another **Learning Objective** is a practical understanding of real-world impacts of these laws and regulations on the daily activities of corporations, individuals, businesses and litigation. You will learn how to apply the concepts and analytical modalities we discuss in class, and you read in the assigned materials, in drafting exercises that will include preparation of discovery requests and responses; internal memoranda; information governance policies and procedures; motions to compel discovery and to preclude the introduction of electronic evidence and social media policy training materials. This is a “practice-ready” course, and I will expect you to keep the practical in mind as you read, discuss and think about the theoretical.

Please be advised that this course will challenge you to, as Steve Jobs said, Think Different. You will look at interactions over electronic media in an entirely new way. You will also be asked to analyze legal problems where there is little case law, or where the case law is in conflict, and to prepare pleadings, memoranda, discovery demands and motions that you have never seen before. You will be graded on how you rise to those challenges and hopefully, will leave the class with a unique understanding of one of the most fascinating, and fastest-growing areas of the law. And you will also, I hope, acquire analytical and writing skills that will assist you throughout your career.

COURSE REQUIREMENTS

This course uses a seminar format, and so there will be a great emphasis on informed and well-prepared student participation. **Twenty-five percent of the grade will be based on active and informed class participation. Attendance, therefore, is critical. Seventy-five percent of the grade will be based on students’ performance on five drafting assignments.**

CLASS OVERVIEW, READINGS AND ASSIGNMENTS

NB: Electronic information compliance is an area of law that is still in an evolutionary state. New laws, regulations and/or judicial decisions can change the landscape in a day. Therefore, **the topics for a particular class, and the assignments, may be revised during the semester, though I will provide sufficient notice if this were to occur.**
The law in this area can change overnight, as was seen earlier this year in the Supreme Court's decision in *Riley v. California* (the warrantless cell phone search case).

Reading Assignment for First Class:

Paul, 17-31; 230-258

Riley v. California, available at http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

Week One: Exploration of concepts of protected data: What, how and why.

Reading:

Paul, 155-207

eBay Canada (to be distributed)

The Sedona Guidelines: Best Practices for Managing Information and Records in the Information Age (2007)

Week Two: Overview: Inconsistent compliance schemes between nations and even within the U.S. as the result of clashes of commercial and national cultures, history and legal systems.

Reading:

Paul, 209-229

In re Vitamins Litigation, 120 F.Supp2d 25

Week Three: Chasing the tail: Law, evolving technology and accelerating e-commerce

- a. The blurring of borders due to technology versus the hardening of political borders in response
- b. Overview of information categories and their uses and disclosures in business and law
- c. The proliferation of e-commerce and its effect on jurisdiction (a high-level overview)

Reading:

ABA Resolution 103 Report and Recommendation, to be distributed

In re Payment Card Interchange (to be distributed)

Columbia Pictures v. Bunnell, 2007 WL 2080419

Week Four: Introduction to the international mosaic: why it's different beyond the U.S.

- a. Differing notions of privacy
- b. The influence of history (*i.e.*, experience with authoritarian regimes);
- c. Data protection and sovereign imperatives
- d. Litigation disclosures in civil law systems versus common law

Reading:

Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data

1995 O.J. (L 281) (EC), *available at*

<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

The Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts, pp. 3-29

The Sedona Conference International Principles (EU Edition)

In re Avocat Christopher X (English translation to be distributed)

In re Global Power Equipment Group, 2009 WL 3464212 (Bkrcty.D.Del.)

Week Five: Exploring the international mosaic: categories of laws and regulations affecting the management of ESI

- a. Blocking statutes
- b. Data protection vs. privacy laws
- c. Cyber-security requirements for data transfers
- d. The compliance challenges for U.S.-based multinational organizations and the preparation of data management policies, procedures, training materials and compliance monitoring schemes and documentation

Writing Assignment: Two-page Memorandum on issues of concern for company's revision of cross-border information governance protocols

Reading:

Pension Committee v. Banc of America Sec., 685 F.Supp 2d 456 (SDNY 2010)

Chin v. Port Authority of New York & New Jersey, --- F.3d ---, 2012 WL 2760776 (2d Cir. July 10, 2012),

WP 158 (to be distributed)

"US Legal Holds Across Borders: A Legal Conundrum?", to be distributed

Week Six: International e-discovery 101: Preservation

- a. Preservation and the Litigation Hold across borders
- b. Potential conflicts between U.S. requirements and non-U.S. laws (*i.e.*, laws in Korea and Brazil that mandate deletion after the purpose for which the personal data has been collected has been fulfilled)
- c. Writing Assignment: Preparation of discovery request and response (students divided into proponent and respondent)

Reading:

Aerospatiale v. District Court of Iowa, 482 U.S. 522 (1987)

Wultz v. Bank of China, 2012 WL 5378961 (SDNY Oct. 29, 2012)

“Scaling the Virtual Tower of Babel: Legal Historical and Cultural Challenges to Cross-Border Data Flows,” The Sedona Conference (to be distributed)

Week Seven: International e-discovery 102: Collection, production, international comity and potential conflicts with U.S. laws

- a. Discovery (common-law systems v. Disclosure (civil law))
- b. EU mandates for pre-collection culling and filtering of irrelevant and sensitive personal data
- c. *Aerospatiale v. District Court of Iowa* five-factor balancing test for U.S. courts to consider and follow and-U.S. laws relating to discovery
- d. Practical steps: when to bring up conflicts of law; how to raise the issues to adversaries, judges and governmental agencies; motions to quash subpoenas and for protective orders
- e. Treaty procedures: Hague Convention on Taking Evidence Abroad
- f. Ethical considerations and minefields: lessons from *Qualcomm v. Broadcom*

Writing Assignment: Preparation of motion for Protective Order or Opposition (students divided into movant and opponent)

Reading:

HIPAA Omnibus Final Rule, pp. 2-5; 25-48; 492-543, available at <http://federalregister.gov/a/2013-01073>

Massachusetts 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH (to be distributed)

Week Eight: U.S. ESI Compliance Part One: Federal and State Compliance Statutory and Regulatory Overview for Healthcare ESI

- a. HIPAA and related federal statutes and regulations (healthcare will be addressed extensively in the next class)

- b. Industry-specific laws and regulations overview (finance will be discussed here and in greater detail in a subsequent class)
- c. Children's Online Privacy Protection Act
- d. Writing Assignment: Short slide deck (five slides) for training on health information protocols

Reading:

California Confidentiality of Medical Information Act, CA Civil Codes Sections 56-56.16

Sutter Health et al. v. The Superior Court of Sacramento County, available at

<http://www.courts.ca.gov/opinions/documents/C072591.PDF>

Mott v. Nassau University Medical Center, 2011 NY MISC LEXIS 4622

Week Nine: U.S. Health Information Compliance, Part Two

- a. HIPAA Security and Privacy Rules: analysis and practical compliance challenges
- b. State laws may be stricter than HIPAA: *i.e.*, New York, California, Massachusetts, North Carolina and Texas
- c. Dept. of Health and Human Services commentaries, Guidances, FAQ responses and decisions in HIPAA administrative proceedings
- d. State Departments of Health
- e. Angels in the architecture: design of electronic medical records systems to avoid liability exposures
- f. Writing Assignment: Draft a 3-page social media policy for a hospital

Reading:

SEC Cyber-Security Risk Alert April 15, 2014 (to be provided)

U.S. Federal Trade Commission v. Wyndham Worldwide Corp., Complaint, to be distributed

Week Ten: Financial Electronic Information Compliance

- a. Gramm-Leach Bliley Act
- b. Foreign Corrupt Practices Act
- c. U.K. Bribery Act
- d. U.S. Patriot Act
- e. SEC regulations
- f. Sarbanes-Oxley Act (Section 404 controls over assets, including information assets)
- g. Payment Card Interchange rules

Reading:

In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation., 2014 WL 1661004, at *5 (S.D.N.Y. April 25, 2014)

In the Matter of a Warrant for All Content and Other Information Associated With the Email Account xxxxx@gmail.com, Maintained at Premises E-mail Account Controlled BY Google, Inc., 14 Mag. 309 (SDNY, Magistrate Judge Gorenstein, July 18, 2014) (to be provided)

Rashbaum, Kenneth N., Borden, Bennett B. and Beaumont, Theresa H., "Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing," *Ave Maria Law Review*, 12 Ave Maria L. Rev. 71 (2014)

Week Eleven: Cyber-Security and The Cloud

- a. International compliance for Cloud services (*i.e.*, registration with local data protection authorities, security levels, etc.)
- b. Health information in the Cloud
- c. The Service Level Agreement (Cloud contract): review, critical elements, negotiation
- d. State and federal laws affecting providers and users (Stored Communications Act, etc.)

Reading:

Lorraine v. Markel American Insurance Co., 2007 U.S.

Dist. LEXIS 33020 (D. Md. May 4, 2007)

Kenneth N. Rashbaum, Matthew F. Knouff & Dominique Murray, *Admissibility of Non-U.S. Electronic Evidence*, XVIII RICH. J. L. & TECH. 9 (2012),

<http://jolt.richmond.edu/v18i3/article9.pdf>

Paul, 31-49; 113-129

Week Twelve: Litigation and Arbitration: admissibility of ESI

- a. Evidentiary foundation and how to meet it with various types of ESI
- b. ESI from outside the U.S.: challenges in authentication, reliability and establishing a business records exception to the Hearsay Rule
- c. The litigator and arbitrator's prime directive: educating the court on the technology and substance

Writing Assignment: Motion *in limine* to preclude electronic evidence, or Opposition

Reading:

Scott v. Beth Israel Medical Center, 17 Misc.3d 934, 847 N.Y.S.2d 436

(S. Ct. N.Y. 2007)

Steingart v. Loving Care Agency (to be provided)

United States v. Finazzo, 2013 WL 619572

Qualcomm v. Broadcom, 2008 WL 66932

Week Thirteen: Proceed With Great Care: Privilege and Ethical Potholes in Electronic Communications

- a. Counseling clients on uses and disclosures of their business information in the Digital Age: avoiding ethical dilemmas and land mines
- b. Privilege as a fragile thing that can be lost by client or counsel
 - a. Effect of NSA “snooping” and Google’s admission that it reads Gmails. Does either of these facts cause a waiver of privilege?
 - b. Clawbacks and FRE Rule 506