**CERTIFIED INFORMATION PRIVACY PROFESSIONAL/UNITED STATES**
**NORTHERN VIRGINIA COMMUNITY COLLEGE**
**RESTON, RESTON TECH TRAINING CENTER**
**AND**
**ON-LINE**
**WED, FEBRUARY 17, 2016 – MARCH 23. 2016: 6:30 – 9:30 PM**
**INSTRUCTOR: MONTGOMERY BLAIR SIBLEY**
**J.D., MASTERS, CYBER SECURITY POLICY, CIPP/US**
**Tuition: $489.00**

There's a real need for professionals who know the issues and impacts of data privacy. Whether you work in the public or private sector, this course teaches you the privacy know-how you need to successfully steward the Personal Identifiable Information (PII) in your organization. The Course will prepare the student to take and pass the Certified Information Privacy Professional/United States (CIPP/US) credential granted by the International Association of Privacy Professionals. The CIPP/US confirms that you know privacy laws and regulations and how to apply them thus securing your place in the information economy.

Additionally, each week a case-study of privacy in contemporary privacy issues will be analyzed. These case-studies will include privacy issues raised in : (i) The Elizabeth Duke Fugitive case, (ii) D.C. Madam Escort Service Case, (iii) The All Funds $35 million seizure case, (iv) The Barack Obama Identity Document litigation cases, and (v) Motivated-Intruder threats to Corporations.

A Syllabus for the course follows:

## WEEK 1/FEBRUARY 17, 2016
## MODULE #1

I. Why Privacy Matters: Overview of Current Issues

A. Current Issues

1. Zip Codes & Personally Identifiable Information ("PII")
2. Shredding Documents and PII
3. Social Media & National Labor Relations Act
4. EU & US – Safe Harbor
5. Losing PII
6. Target & Lawyers
7. Cybersecurity Information Sharing Act of 2015 (CISA)

B. Implementing Privacy Compliance Requirements – Privacy Impact Assessments

1. Asset Management
2. Governance
3. Risk Assessment
4. Risk Management Strategy
5. Access Control
6. Awareness & Training
7. Data Security
8. Information Protection & Procedures
9. Protective Technology

II. Introduction to the U.S. Privacy Environment

A. Structure of U.S. Law

1. Branches of government – Legislative, Executive, Judicial
2. Sources of law
    i. Constitutions
    ii. Legislation
    iii. Regulations and rules
    iv. Case law
    v. Common law
    vi. Contract law
3. Legal definitions
    i. Jurisdiction
    ii. Person
    iii. Preemption
    iv. Private right of action
4. Regulatory authorities
    i. Federal Trade Commission (FTC)
    ii. Federal Communications Commission (FCC)
    iii. Department of Commerce (DoC)
    iv. Department of Health and Human Services (HHS)
    v. Banking regulators
        1. Federal Reserve Board
        2. Comptroller of the Currency
    vi. State attorneys general
    vii. Self-regulatory programs and trust marks
5. Understanding laws
    i. Scope and application
    ii. Analyzing a law
    iii. Determining jurisdiction
    iv. Preemption

B. Enforcement of U.S. Privacy and Security Laws

1. Criminal versus civil liability
2. General theories of legal liability
    i. Contract
    ii. Tort
    iii. Civil enforcement
3. Negligence
4. Unfair and deceptive trade practices (UDTP)
5. Federal enforcement actions
6. State enforcement (Attorneys General (AGs), etc.)
7. Cross-border enforcement issues (Global Privacy Enforcement Network (GPEN))
8. Self-regulatory enforcement (PCI, Trust Marks)

**C. The Elizabeth Duke Fugitive case**

**1. Background – The bombings**
**2. Indictment/Arraignment/Flight**
**3. Dismissal/Forgery**
**4. Investigation/Litigation/Appeal**

D. Information Management from a U.S. Perspective

1. Data classification
2. Privacy program development
3. Incident response programs
4. Training
5. Accountability
6. Data retention and disposal (FACTA)
7. Vendor management
8. Vendor incidents
9. International data transfers
    i. U.S. Safe Harbor
    ii. Binding Corporate Rules (BCRs)
10. Other key considerations for U.S.-based global multinational companies
11. Resolving multinational compliance conflicts
    i. EU data protection versus e-discovery

**WEEK 2/FEBRUARY 24, 2016**
**MODULE #2**

I. Limits on Private-sector Collection and Use of Data

A. Cross-sector FTC Privacy Protection

1. The Federal Trade Commission Act

2. FTC Privacy Enforcement Actions
3. FTC Security Enforcement Actions
4. The Children's Online Privacy Protection Act of 1998 (COPPA)

B. Medical

1. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
   i. HIPAA privacy rule
   ii. HIPAA security rule
2. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

C. Financial

1. The Fair Credit Reporting Act of 1970 (FCRA)
2. The Fair and Accurate Credit Transactions Act of 2003 (FACTA)
3. The Financial Services Modernization Act of 1999 ("GLBA")
   i. GLBA privacy rule
   ii. GLBA safeguards rule
4. Red Flags Rule
5. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010
6. Consumer Financial Protection Bureau

D. Education

1. Family Educational Rights and Privacy Act of 1974 (FERPA)
2. **The Barack Obama Identity Document litigation cases**
   **i. Background & Documents**
   **ii. Litigation for College & University Records**

E. Telecommunications and Marketing

1. Telemarketing sales rule (TSR) and the Telephone Consumer Protection Act of 1991 (TCPA)
   i. The Do-Not-Call registry (DNC)
2. Combating the Assault of Non-solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
3. The Junk Fax Prevention Act of 2005 (JFPA)
4. The Wireless Domain Registry
5. Telecommunications Act of 1996 and Customer Proprietary Network Information
6. Video Privacy Protection Act of 1988 (VPPA)
7. Cable Communications Privacy Act of 1984

**WEEK 3/MARCH 2, 2016**
**MODULE #3**

I. Government and Court Access to Private-sector Information

A. Law Enforcement and Privacy

1. Access to financial data
   i. Right to Financial Privacy Act of 1978
   ii. The Bank Secrecy Act
2. Access to communications
   i. Wiretaps
   ii. Electronic Communications Privacy Act (ECPA)
      1. E-mails
      2. Stored records
      3. Pen registers
3. The Communications Assistance to Law Enforcement Act (CALEA)

**4. The All Funds $35 million seizure case**
   **i. Background of seizures**
   **ii. Government warrant-less seizures**
   **iii. Litigation & Result**

B. National Security and Privacy

1. Foreign Intelligence Surveillance Act of 1978 (FISA)
   i. Wiretaps
   ii. E-mails and stored records
   iii. National security letters
2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA-Patriot Act)
   i. Other changes after USA-Patriot Act

C. Civil Litigation and Privacy

1. Compelled disclosure of media information
   i. Privacy Protection Act of 1980
2. Electronic discovery

**WEEK 4/MARCH 9**
**MODULE #4**

I. Workplace Privacy

A. Introduction to Workplace Privacy

1. Workplace privacy concepts
    i. Human resources management
2. U.S. agencies regulating workplace privacy issues
    i. Federal Trade Commission (FTC)
    ii. Department of Labor
    iii. Equal Employment Opportunity Commission (EEOC)
    iv. National Labor Relations Board (NLRB)
    v. Occupational Safety and Health Act (OSHA)
    vi. Securities and Exchange Commission (SEC)
3. U.S. Anti-discrimination laws
    i. The Civil Rights Act of 1964
    ii. Americans with Disabilities Act (ADA)
    iii. Genetic Information Nondiscrimination Act (GINA)

B. Privacy before, during and after employment

1. Employee background screening
    i. Requirements under FCRA
    ii. Methods
        a. Personality and psychological evaluations
        b. Polygraph testing
        c. Drug and alcohol testing
        c. Social media
2. Employee monitoring
    i. Technologies
        a. Computer usage (including social media)
        b. Location-based services (LBS)
        c. Mobile computing
        d. E-mail
        e. Postal mail
        f. Photography
        g. Telephony
        h. Video
    ii. Requirements under the Electronic Communications Privacy Act of 1986 (ECPA)
    iii. Unionized worker issues concerning monitoring in the U.S. workplace
3. Investigation of employee misconduct

i. Data handling in misconduct investigations
ii. Use of third parties in investigations
iii. Documenting performance problems
iv. Balancing rights of multiple individuals in a single situation

4. Termination of the employment relationship
i. Transition management
ii. Records retention
iii. References

**II. Motivated-Intruder threats to Corporations**

**WEEK 5/MARCH 16, 2016**
**MODULE #5**

I. State Privacy Laws

A. Federal vs. state authority

B. Marketing laws

C. Financial Data

1. Credit history
2. California SB-1

D. Data Security Laws

1. SSN
2. Data destruction

E. Data Breach Notification Laws

1. Elements of state data breach notification laws
2. Key differences among states today

**II. Privacy Issues in the D.C. Madam Escort Case**

**A. Background of Case**

**1. Harland Ullman**
**2. Senator David Vitter**
**3. USAID Administrator Randall Tobias**
**4. Escorts**
**5. Clients**

**B. Postal/FedEx Surveillance**
**C. Telephone Records**
**D. Court Orders**

## WEEK 6/MARCH 23, 2016
## MODULE #6

I. CIPP/US Exam Review and Practice Exam