



METRO NYC CHAPTER



Long
Island
Chapter



Innovation & Inspiration
RIM & IG – The Time is NOW!

ARMA Metro NYC
Annual Spring Conference

Tuesday, March 8th, 2016
New York Executive Conference Center
1601 Broadway, New York, NY 10019

Information Sprawl and Data Loss
Prevention

Heidi L. Wachs, Special Counsel
Jenner & Block

Introduction & Outline

- Information Sprawl
 - How did we get here?
 - Why is it a problem?
- How do we control Information Sprawl?
- Information Classification, Records Retention & Data Loss Prevention (DLP)
- Questions



Long
Island
Chapter



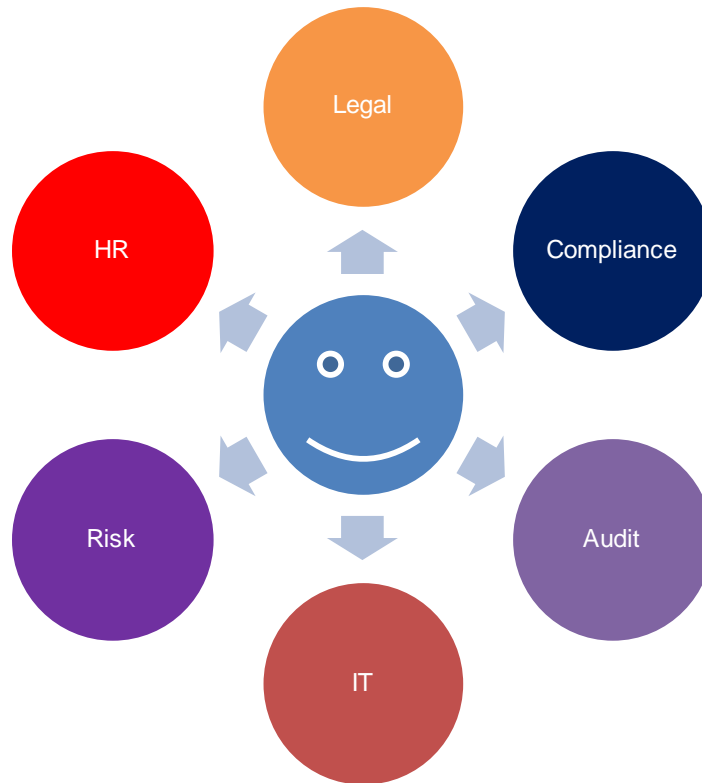
Information Sprawl: How did we get here?



Long
Island
Chapter



Who's the Boss?

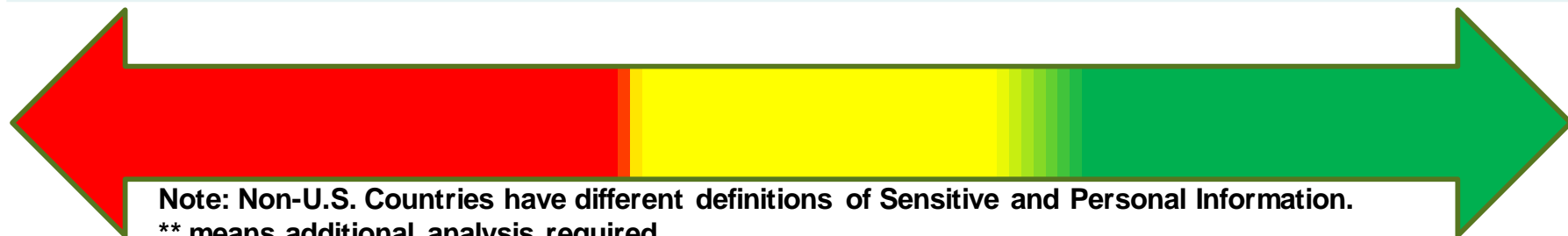


Long
Island
Chapter



METRO NYC CHAPTER

Sensitive Personal Information	Personal Information	Non-Personal Information
Social Security Number	Name (first and last, first initial last name)	First Name
Health Information	User Name (if real name is used)	Zip Code **
Financial Information	Phone Number	City
Age (Children under 13)	Email Address	Aggregate Usage Data
Political Affiliation or union trade membership	Mailing Address	Unique Identifier **
Racial or Ethnic Information	Geo-location**	Cable Provider
Sexual Orientation	IP Address **	
Criminal or Financial Record	Device ID**	



Information Sprawl: Why is it a problem?



Long
Island
Chapter



US Federal & State Statutes, Self-Regulation

- U.S. statutes and regulations:
 - Gramm-Leach-Bliley Financial Privacy Act
 - Fair Credit Reporting Act
 - Children’s Online Privacy Protection Act
 - Electronic Communications Privacy Act
 - Computer Fraud and Abuse Act
 - Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)
 - Telephone Consumer Protection Act
 - CAN-SPAM
 - Video Privacy Protection Act
 - Cable Communications Policy Act (Cable Privacy Act)
 - Family Educational Rights and Privacy Act
- Industry Self-Regulation
- State Laws:
 - 47 Data breach notification laws
 - “Wiretap” laws, two party consent states
 - Medical privacy laws
 - Privacy Policy Law (CA)
 - Shine the Light (CA)
 - Eraser Law for Minors (CA)
 - Data security laws (e.g., MA)
 - Unfair and deceptive trade practices



Long
Island
Chapter



State Laws

- Data breach notification statutes
 - These are really data security laws
- California Online Privacy Protection Act
 - Requires disclosure of data collection practices
- Connecticut General Statutes § 42-471
 - Requires that holders of another’s personal information must “safeguard the data, computer files and documents containing the information from misuse by third parties”
- Massachusetts Regulation 201
 - Imposes duty to select and retain service providers that can maintain appropriate security measures



Long
Island
Chapter



Data Breach Notification Laws

- Overview of state approaches to data breach
 - 47 states and District of Columbia (no AL, NM, SD)
 - Generic definition of personal information: An individual's first name or first initial and last name plus one or more of following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account.
 - **New Trend (CA, FL, WY, etc) – user name and password breach now requires notification**
 - Frequent requirement to report to state official/AG
 - Encryption of data a safe harbor except in WY, GA (but these states are risk-based standards)
- A handful of states have private rights of action (AK, CA, DC, LA, MD, MN, NH, NC, SC, TN, WA) for non-notification



Long
Island
Chapter



Global Laws and Regulations

- Privacy and Data Protection Laws
 - EU Data Protection Directive (proposed regulation)
 - APEC
 - Trans Border Data Flow
- Export Control Laws
 - ITAR, Global Trade
 - Trans Border Data Flow



Long
Island
Chapter



How do we control Information Sprawl?



Long
Island
Chapter



Data Inventories

- Understanding what the company has, and where it has it
- Catalog repositories of company data
 - Start with high risk or high volume applications or systems
- Use the method most amenable to your company
 - Surveys
 - Brain trust
 - Self-assessment
- Don't neglect cloud-based or hosted solutions



Long
Island
Chapter



Privacy Impact Assessments

- Channel your inner 5 year old: Why, Why, Why???
 - What data is being collected?
 - Is the data regulated?
 - Why is it being collected?
 - Where is it being stored?
 - How is it protected?
 - Who will access it?
 - When will it be destroyed?
- Proactive: assess new systems, applications, whether hosted or on-premises
- Reactive: assess existing systems and applications at time of upgrade or contract renewal



Long
Island
Chapter

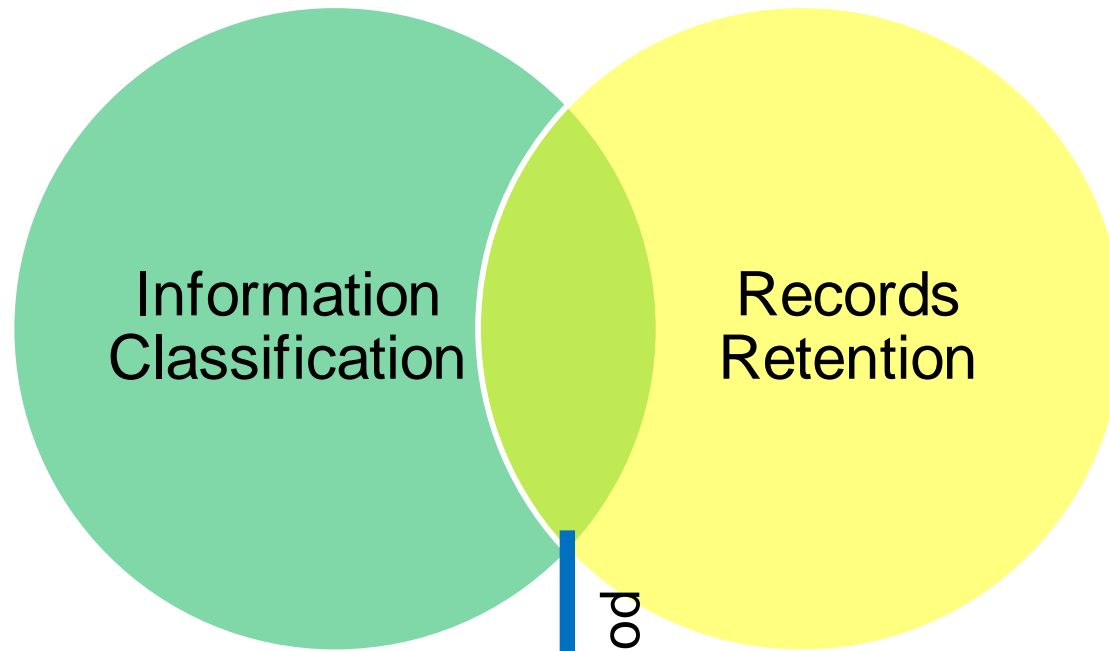


Information Classification, Records Retention, and DLP



Long
Island
Chapter





DLP



Long Island Chapter



METRO NYC CHAPTER



Information Classification

- Two basic components:
 - 1) Analyze your data assets
 - 2) Organization of those assets into categories
 - Sensitivity, legal restrictions, business interests, etc.
- Good info. class is systematic and repeatable
 - Common requirements, needs, etc. across different types of data, in order to simplify your information management program



Long
Island
Chapter



Sample Information Classification Scheme

Restricted

- Social Security Numbers
- ePHI (HIPAA)
- Cardholder Data (PCI)

Confidential

- Intellectual Property
- Addresses, demographic info, etc.
- Contracts

Internal

- Business Plans
- Other proprietary information
- Must move freely within company

Public

- Press releases
- Marketing materials
- Other materials intended for public consumption



Long
Island
Chapter



What is Records Retention?




- Operational:
 - specific, below the “policy level”
 - not dependent on data classifications
- Not specifically focused on data security
- In many companies, handled by Records Management team, not Privacy or Info Security functions
 - But may be part of a larger Enterprise Compliance group



Long
Island
Chapter



Sample Records Retention Schedule

 LIBRARY OF VIRGINIA ARCHIVAL AND RECORDS MANAGEMENT SERVICES DIVISION (RM-2 Form August 2011)			RECORDS RETENTION AND DISPOSITION SCHEDULE GENERAL SCHEDULE NO. 12 CIRCUIT COURT RECORDS		
EFFECTIVE SCHEDULE DATE: November 21, 2011		SUPERSEDES SCHEDULE DATED: June 17, 2008		PAGE 4 OF 25 PAGES	
RECORDS SERIES AND DESCRIPTION	SERIES NUMBER	SCHEDULED RETENTION AND DISPOSITION			
<u>Bond Books – Post-1912</u> This series documents bonds taken of officers, executors, administrators, trustees, or other fiduciaries and all bonds of commissioners and receivers; all suspending, appeal, injunction, attachment, and cost bonds; all other bonds required to be recorded. Refer to <i>Code of Virginia</i> , §17.1-230.	010443	Retain permanently.			
Defunct Series <u>Capitation Tax Books, Paid and Delinquent</u> This series documents poll tax imposed on individuals.	010444	Retain permanently.			
<u>Cases, Civil – Habitual Offender</u> This series consists of cases pertaining to declarations of habitual offender status and full restoration of driving privileges.	010445	Retain 10 years then destroy (<i>Code of Virginia</i> , §17.1-213 (B) (13)).			
<u>Case Papers, Civil, District Court – Prior to Jan. 1, 1985</u> This series consists of district court cases concerning civil or private rights and remedies. May include warrants in debt and unlawful detainers. Refer to <i>Code of Virginia</i> , §16.1-116, 16.1-69.58.	010446	Retain 20 years after judgment; if there is no motion to extend, then destroy (<i>Code of Virginia</i> , §16.1-118). Or, destroy if: (1) Retained for 1 year after order of dismissal. (2) Judgment is barred. (3) There is no service of warrant or motion or other process or summons on any defendant, and 1 year has elapsed from the date of such process or summons. (4) Ordered by the judge.			
<u>Cases, Ended Chancery and Law – Pre-1913</u> This series consists of cases administered according to system of equity and/or common law procedure. Includes pleadings and orders.	010447	Retain permanently in hard copy form in locality or in Archives, Library of Virginia (<i>Code of Virginia</i> , §17.1-213 (A)).			



Long
Island
Chapter



METRO NYC CHAPTER

Data Loss Prevention (DLP)

- Implements technical policies, as defined by your company, to scan and block certain data elements or key words from transmission
- Can be tied to information classification schemes and labeling tools
- Many DLP tools can be used proactively, but also applied retroactively to search and classify existing repositories



Long
Island
Chapter



METRO NYC CHAPTER

Not Everyone Loves DLP

- Is my company spying on me?
- Ignorance is bliss
- Newfound data = newfound obligations?
- This is not how we do things



Long
Island
Chapter



QUESTIONS?



Long
Island
Chapter

