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
Information Sprawl: How did we get here?
Who’s the Boss?
<table>
<thead>
<tr>
<th>Sensitive Personal Information</th>
<th>Personal Information</th>
<th>Non-Personal Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>Name (first and last, first initial last name)</td>
<td>First Name</td>
</tr>
<tr>
<td>Health Information</td>
<td>User Name (if real name is used)</td>
<td>Zip Code **</td>
</tr>
<tr>
<td>Financial Information</td>
<td>Phone Number</td>
<td>City</td>
</tr>
<tr>
<td>Age (Children under 13)</td>
<td>Email Address</td>
<td>Aggregate Usage Data</td>
</tr>
<tr>
<td>Political Affiliation or union trade membership</td>
<td>Mailing Address</td>
<td>Unique Identifier **</td>
</tr>
<tr>
<td>Racial or Ethnic Information</td>
<td>Geo-location**</td>
<td>Cable Provider</td>
</tr>
<tr>
<td>Sexual Orientation</td>
<td>IP Address **</td>
<td></td>
</tr>
<tr>
<td>Criminal or Financial Record</td>
<td>Device ID**</td>
<td></td>
</tr>
</tbody>
</table>

Note: Non-U.S. Countries have different definitions of Sensitive and Personal Information. ** means additional analysis required.
Information Sprawl: Why is it a problem?
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
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
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
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
How do we control Information Sprawl?
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
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
Information Classification, Records Retention, and DLP
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 \textit{systematic} and \textit{repeatable}
  – Common requirements, needs, etc. across different types of data, in order to simplify your information management program
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
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
# Sample Records Retention Schedule

## Records Retention and Disposition Schedule

**General Schedule No. 12**

**Circuit Court Records**

<table>
<thead>
<tr>
<th>RECORDS SERIES AND DESCRIPTION</th>
<th>SERIES NUMBER</th>
<th>SCHEDULED RETENTION AND DISPOSITION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bond Books – Post-1912</strong>&lt;br&gt;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 <em>Code of Virginia</em>, §17.1-230.</td>
<td>010443</td>
<td>Retain permanently.</td>
</tr>
<tr>
<td><strong>Defunct Series</strong>&lt;br&gt;Capitation Tax Books, Paid and Delinquent&lt;br&gt;This series documents poll tax imposed on individuals.</td>
<td>010444</td>
<td>Retain permanently.</td>
</tr>
<tr>
<td><strong>Cases, Civil – Habitual Offender</strong>&lt;br&gt;This series consists of cases pertaining to declarations of habitual offender status and full restoration of driving privileges.</td>
<td>010445</td>
<td>Retain 10 years then destroy (<em>Code of Virginia</em>, §17.1-213 (B) (13)).</td>
</tr>
<tr>
<td><strong>Case Papers, Civil, District Court – Prior to Jan. 1, 1985</strong>&lt;br&gt;This series consists of district court cases concerning civil or private rights and remedies. May include warrants in debt and unlawful detainers. Refer to <em>Code of Virginia</em>, §16.1-116, 16.1-69.58.</td>
<td>010446</td>
<td>Retain 20 years after judgment; if there is no motion to extend, then destroy (<em>Code of Virginia</em>, §16.1-118).&lt;br&gt;Or, destroy if:&lt;br&gt;(1) Retained for 1 year after order of dismissal.&lt;br&gt;(2) Judgment is barred.&lt;br&gt;(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.&lt;br&gt;(4) Ordered by the judge.</td>
</tr>
<tr>
<td><strong>Cases, Ended Chancery and Law – Pre-1913</strong>&lt;br&gt;This series consists of cases administered according to system of equity and/or common law procedure. Includes pleadings and orders.</td>
<td>010447</td>
<td>Retain permanently in hard copy form in locality or in Archives, Library of Virginia (<em>Code of Virginia</em>, §17.1-213 (A)).</td>
</tr>
</tbody>
</table>
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
Not Everyone Loves DLP

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