Emerging Privacy and Cybersecurity Issues

Andrew Serwin
CEO, The Lares Institute
Partner, Morrison & Foerster LLP
aserwin@mofo.com
Overview

• The growing role of information in companies.
  • There are more transactions that depend upon information and brand;
  • We are creating more information; and
  • We are reviewing little of the actionable information.

• The importance of privacy.
  • Why does it matter?
  • What is it?

• Cybersecurity.
Tools for Discussion Today

- Privacy 3.0—The Principle of Proportionality.
  - This creates a data classification system similar to the intelligence structure, but based upon consumer and private sector information.

- Information Superiority.
  - This is a DoD tool that can be used by the private sector to help govern information.
The Problem of “Big Data”
Executive Decision-Making

• “The job of a manager is, above all, to make decisions. At any moment in any day, most executives are engaged in some aspect of decision making: exchanging information, reviewing data, coming up with ideas, evaluating alternatives, implementing directives, following up.

... To climb the corporate ladder and be effective in new roles, managers need to learn new skills and behaviors—to change the way they use information and the way they create and evaluate options.”

Information Is a Strategic Asset

- Information is no longer the byproduct of other business activity.
  - Entire business models exist based upon the collection and processing of information.
  - As more transactions move online, information becomes more critical.
  - Companies are gathering more information and trying to understand their customers better.
  - The innovation economy in the United States utilizes a significant amount of information.
- Process improvement depends upon information.
- New forms of marketing depend upon information.
Examples of Information

• Your company creates, gathers, and processes a significant amount of information:
  • Financial information;
  • Information regarding individuals (employees, customers, or both);
  • Proprietary/confidential information
    • Undisclosed M&A activity;
    • Business and marketing plans; and
    • Pricing;
  • IP;
  • Information regarding businesses processes, including process improvements;
  • Information regarding business trends;
  • Social data/user-generated content;
  • Machine data; and
  • Many other forms of information.
What Information Does Your Company Have?

- Non-public proprietary: 91.7%
- Customer contact information: 91.7%
- Credit card: 83.3%
- SSN: 83.3%
- Health information: 75.0%
- Consumer financial information: 58.3%
- Location-based data: 58.3%
- Purchase history: 50.0%
- Driver’s license number: 50.0%
- Search or browsing history: 41.7%
- Biometric: 33.3%
- Genetic: 25.0%
How Much Information Are We Creating and Storing?

- 500 gigabytes (or .5 terabyte)—your laptop’s hard drive.
- 10 terabytes (20 laptops)—the entire Library of Congress (only books).
- 2 petabytes (4,166 laptops)—all U.S. academic research libraries.
- 1.8 zetabytes (4.5 billion laptops)—the total amount of information we created in 2011. This grew by a factor of nine in five years.
- It is believed that this will grow by a factor of 50 by 2020.
What Are We Doing with the Information?

- 23% of the data created would be useful, were it to be analyzed.
- Less than 1% of the available information is analyzed.
- In other words, we keep gathering more information, but we are not systematically reviewing it, and no one is in charge of it.
Information Imbalances—9/11

• “In each of our examples, no one was firmly in charge of managing the case and able to draw relevant intelligence from anywhere in the government, assign responsibilities across the agencies (foreign or domestic), track progress, and quickly bring obstacles up to the level where they could be resolved. Responsibility and accountability were diffuse.”

• “The agencies cooperated, some of the time. But even such cooperation as there was is not the same thing as joint action. When agencies cooperate, one defines the problem and seeks help with it. When they act jointly, the problem and options for action are defined differently from the start. Individuals from different backgrounds come together in analyzing a case and planning how to manage it.”

• “In our hearings we regularly asked witnesses: Who is the quarterback? The other players are in their positions, doing their jobs. But who is calling the play that assigns roles to help them execute as a team?”
What Are the Consequences?

• Information imbalances are created that can create competitive and legal risk for companies, including as a result of privacy issues.
• These information imbalances also increase costs and reduce profits.
• In short, Big Data can prevent your company from “connecting the dots.”
Why Does Privacy Matter?
In the Last 12 Months, Have You Made a Decision Regarding What Company to Purchase Products or Services from Based upon Concerns over Privacy?

- Yes: 60.9%
- No: 39.1%
In the Last 12 Months, Have You Made a Decision Regarding What Company to Purchase Products or Services from Based upon Concerns over Privacy?—By Sensitivity

- Low: 5%
- Medium: 40%
- High: 54%
What is Privacy?

• Privacy is a societal norm (that is sometimes contained in laws) that expresses limitations over the collection, protection, processing, and deletion of information regarding an individual.

• Privacy presents risk for your company.
  • Business risks of privacy—including loss of trust.
  • Legal risks of privacy.
Demographics and Sensitivity

• If privacy is a societal norm, factors other than the law can impact privacy.
Demographics

• Relevant demographic factors include:
  • Age;
  • Income; and
  • Education.
Privacy Sensitivity by Age

[Bar chart showing privacy sensitivity by age group, with percentages for Low, Medium, and High.
- Under 18-25: 11%, 67%, 79%
- 26-45: 6%, 16%, 75%
- 46-65: 4%, 13%, 83%
- 66+: 10%, 15%, 75%]
Privacy Sensitivity—Health by Age

![Bar Chart]

- **Low**:
  - Under 18-25: 24%
  - 26-45: 17%
  - 46-65: 21%
  - 66+: 24%

- **Medium**:
  - Under 18-25: 16%
  - 26-45: 16%
  - 46-65: 15%
  - 66+: 51%

- **High**:
  - Under 18-25: 67%
  - 26-45: 63%
  - 46-65: 75%
  - 66+: 63%
Privacy Sensitivity—Health by Income
Have You Read the Privacy Policies You Receive from Your Health Care Providers? By Income.
Have You Read the Privacy Policies You Receive from Your Internet Service Provider? By Education.

- Yes: 44% (No College Degree), 26% (College or Graduate Degree)
- No: 39% (No College Degree), 27% (College or Graduate Degree)
- Some of them: 24% (No College Degree), 29% (College or Graduate Degree)
- I am unaware whether I receive these privacy policies: 3% (No College Degree), 3% (College or Graduate Degree)
- I have not received any such policies: 2% (No College Degree), 3% (College or Graduate Degree)
Why Are People Concerned about Privacy?

- Identity theft: 20%
- There really is no privacy anymore: 10%
- People can steal information if they want to: 9%
- I chose to be private; it is a right: 8%
- I am concerned over government monitoring: 7%
- You have to balance the risks and rewards: 7%
Why Do People Trust Companies with Their Information?

- 27% Trust in brand or technology
- 19% No company is perfect
- 13% Observed Technology
- 12% Long term customer
- 8% Heavily regulated

No company is perfect.
Why Do People Trust Companies with Their Information?

- Researched the company: 6%
- Read the policies: 5%
- Never had a problem: 5%
- Had an issue and it was addressed: 3%
- Financial Space: 1%
Top 5 Reasons for Trust by Sensitivity

- Trust in brand or technology: 44%
- No company is perfect: 27%
- Observed Technology: 22%
- Long term customer: 16%
- Heavily regulated: 10%
Whom Do You Trust More?
Before Snowden

- Government: 29.8%
- Private Companies: 29.0%
- I trust them equally: 41.3%
Trust by Age

Government
- Under 18-25: 33%
- 26-45: 28%
- 46-65: 24%
- 66+: 33%

Private companies.
- Under 18-25: 15%
- 26-45: 23%
- 46-65: 33%
- 66+: 44%

I trust them both equally.
- Under 18-25: 52%
- 26-45: 44%
- 46-65: 39%
- 66+: 32%

Under 18-25 | 26-45 | 46-65 | 66+
---|---|---|---
Government | 33% | 28% | 24% | 33%
Private companies | 15% | 23% | 33% | 44%
I trust them both equally | 52% | 44% | 39% | 32%
What Happens When We Get It Wrong?
Has Your Trust in Government Changed?

- It has increased: 1.7%
- It has decreased: 38.6%
- It has stayed the same: 49.8%
- I don’t know what allegations have been made: 10.0%
Whom Do You Trust More?—Post-Snowden

Chart Title

- Government: Pre-Snowden 29.8%, Post-Snowden 19.7%
- Private Companies: Pre-Snowden 29.0%, Post-Snowden 35.0%
- I trust them equally: Pre-Snowden 41.3%, Post-Snowden 45.4%
Data Element Sensitivity

• Key points.
  • A person’s stated sensitivity is consistent with the data element sensitivity.
  • Sensitivity rankings are not consistent across the three levels of sensitivity.
  • There are some surprises regarding what people find to be sensitive.
Stated Sensitivity Is Consistent with Data Element Sensitivity

- 78% of the data elements showed statistically significant variances in sensitivity that were consistent with the respondents’ general sensitivity.
Stated Sensitivity Is Consistent with Data Element Sensitivity—example

Payment card information

<table>
<thead>
<tr>
<th>Level</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>8.40</td>
</tr>
<tr>
<td>Medium</td>
<td>8.82</td>
</tr>
<tr>
<td>High</td>
<td>9.43</td>
</tr>
</tbody>
</table>
Top 10 Most Sensitive Elements

1. Social Security number. (3, 2, 1.)
2. Password or other personal identification number required to access an account or services. (2, 1, 2.)
3. Credit card or other account number, including information associated with a credit card. (1, 4, 3.)
4. Financial information, including income tax filings, and financial statements. (8, 6, 4.)
5. Any ID or number assigned to an individual, including account numbers, user IDs, or passwords. (5, 3, 5.)
6. Payment card information (debit or credit card). (7, 5, 6.)
7. Account balances. (16, 7, 7.)
8. Automated or electronic signatures. (9, 9, 8.)
9. Information from the computer chip, magnetic strip of a credit or other payment card. (4, 10, 9.)
10. Alien registration number, government passport number, employer identification number, taxpayer identification number, Medicaid account number, food stamp account number, medical identification number, or health insurance identification number. (11, 8, 10.)
Bottom 10 Sensitive Data Elements

91. Information regarding marital status. (98, 99, 91.)
92. Occupation. (89, 88, 93.)
93. Purchase history regarding a respondent’s viewing of movies. (100, 91, 90.)
94. Information regarding philosophical beliefs. (91, 97, 94.)
95. Information regarding political beliefs. (96, 98, 95.)
96. Educational history. (97, 95, 96.)
97. What a respondent “likes” on Facebook. (95, 96, 97.)
98. Information regarding religious beliefs. (93, 100, 98.)
99. Information regarding games played online. (83, 92, 99.)
100. Television-viewing information. (99, 94, 100.)
• Generally speaking, marketing and government use for counterterrorism reduce the sensitivity of information.
• For marketing, considering the top 10 most sensitive elements, respondents found these data elements 6.6% less sensitive when used for marketing purposes.
• For use by the government for counterterrorism purposes, respondents found these data elements 13.5% less sensitive.
What Do We Do About Privacy?

- We rely upon already-existing tools to help us address the issues.
Data Classification—Public Sector

• Bases controls, security, and use of the information upon the sensitivity.
• Top Secret
  • Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security, that the original classification authority is able to identify or describe.
• Secret
  • Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security, that the original classification authority is able to identify or describe.
• Confidential
  • Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security, that the original classification authority is able to identify or describe.
• Unclassified.
Privacy 3.0

- Creates four tiers of information.
  - Highly sensitive;
  - Sensitive;
  - Slightly sensitive; and
  - Nonsensitive.
- Bases controls, security, and use of the information upon the sensitivity.
Privacy and Legal Risk

- Government investigations—FTC, state AGs, and others.
- Consumer class actions, which in some cases seek statutory penalties.
- Breaches can impact market capitalization.
- PCI fees and other similar risks.
Privacy—Conclusions

- Privacy is an issue that companies must address;
- Demographics and sensitivity matter; and
- There are public sector tools that can help reduce your risk.
Cybersecurity
Understanding the Cyber Threat

- The cyber threat presents unique issues that are difficult to solve.
Cybersecurity

- Cyberterrorism;
- Organized crime; and
- Industrial espionage.
How Do We Solve Those Issues?

• Identify barriers to information-sharing in the private sector;
  • A lack of horizontal information-sharing;
  • Limitations on executive decision-making;
  • Understand information risks; and
  • Identify emerging threats.

• Identify solutions that increase information-sharing.
Information Superiority

• This is the organizing principle of how the public and private sectors can achieve their goals.
Information Superiority—DoD

- A relative state achieved when a competitive advantage is derived from the ability to exploit an “Information Advantage.”
- The ability to develop and use information while denying an adversary the same capability.
- An Information Advantage is achieved when one competitor outperforms its competitors in the information domain—i.e., when there is an information imbalance.
Information Superiority--DoD

• Sharing has organizational, behavioral, and technical components.
  • Interoperability v. co-operability.
  • Technical component enables.
  • Organizational and behavioral components generate value.
The Private Sector Faces the Same Issues

- No one is in charge of information-sharing;
- Cooperation is not routine;
- Vertical information sharing, not horizontal
  - Are IT, HR, Audit, Legal, Treasury, Security, and others sharing information?
- These issues create challenges for executive decision-making.
Information Superiority—Private Sector

• “Information Superiority” helps businesses achieve the goal of making superior use of information.
• This aids executive decision-making by helping get the right information to the right people at the right time.
The Goal of Information Superiority

- Strategic management of information across the enterprise to:
  - Avoid the next 9/11;
  - Increase profit;
  - Reduce costs;
  - Optimize risk;
  - Reduce the industrial espionage threat; and
  - Reduce brand damage.
Information Superiority

- As in the public sector formulation, there are organizational, technical, and behavioral components.
What Steps Can Be Taken?

- Understand what information you have, and how to avoid an information imbalance;
- Create a governance structure that includes senior stakeholders that are relevant to governing information;
  - Such as IT, HR, Audit, Legal, Treasury, Security, and others.
- Create a framework that classifies your information; and
- Make systematic behavioral changes to how information is collected and processed so that information is shared appropriately with key stakeholders.
Information Sharing—Benchmarking

- [www.laresinstitute.com/benchmarking](http://www.laresinstitute.com/benchmarking)
Annual Revenue

- $100,000,000,000 or more: 4.4%
- $50,000,000,000 or more, but less than $100,000,000,000: 3.5%
- $10,000,000,000 or more, but less than $50,000,000,000: 7.9%
- $1,000,000,000 or more, but less than $10,000,000,000: 11.4%
- $500,000,000, or more, but less than $1,000,000,000: 8.8%
- $100,000,000,000 or more, but less than $500,000,000,000: 17.5%
- $50,000,000,000 or more, but less than $100,000,000,000: 14.9%
- $30,000,000,000 or more, but less than $50,000,000,000: 6.1%
- $10,000,000,000 or more, but less than $30,000,000,000: 4.4%
- $1,000,000,000 or more, but less than $10,000,000,000: 5.3%
- Less than $1,000,000,000: 15.8%
Number of Employees

- More than 20,000: 7.0%
- Between 10,001 and 20,000: 7.0%
- Between 5,001 and 10,000: 12.2%
- Between 1,001 and 5,000: 24.3%
- Between 100 and 1,000: 28.7%
- Less than 100: 20.9%
Are You Located in Southern California?

38.9% Yes. 61.1% No.
## Selected Representative Industries

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications.</td>
<td>ISP.</td>
<td>Real Estate.</td>
<td></td>
</tr>
</tbody>
</table>
What Have You Done in the Last 18 Months?

- A review of information security policies: 56%
- A review of incidents to make changes: 44%
- Benchmarking: 32%
- Audit against ISO: 28%
- Risk assessment: 36%
Other Issues Surveyed

• Security practices.
• Policies and procedures.
• Information sharing.
• Information governance.
• Screening of employees who have access to PII.
• ISO standards.
• Limitations on access to PII.
• Requirements placed on third parties.
• Access controls and encryption.
Conclusions

• Privacy and cybersecurity impact your business.
• Information sensitivity matters.
• There are tools that can help.