

**From PLI's Course Handbook**

*6th Annual Institute on Privacy Law: Data Protection -  
The Convergence of Privacy & Security  
#6080*

48

AN IN-DEPTH LOOK AT THE  
ARCHITECTURE OF AN INFORMATION  
MANAGEMENT PROGRAM:  
PRIVACY, SECURITY & CUSTOMER  
RELATIONSHIP MANAGEMENT IN AN  
AGE OF ID THEFT AND TERRORISM

Margaret P. Eisenhauer  
*Hunton & Williams LLP*

## Biographical Information

**Peggy Eisenhower**, counsel in the Firm's Atlanta office, leads the Hunton & Williams' privacy and information management practice group. She helps companies develop and document privacy and fair information practices, including policies governing the use and distribution of public and non-public data and the use of customer and employee information. She has extensive experience with US and international privacy laws and industry self-regulatory guidelines, and she is a frequent speaker on privacy and information management topics. *Ms. Eisenhower is admitted to practice law in Georgia and Florida.*

## Table of Contents

I.	Introduction.....	7
II.	Managing the Four Privacy & Security Risks .....	8
III.	A Sensible Approach to Fair Information Practices.....	10
IV.	Essential Elements of an Information Management Program.....	11
V.	Conclusions .....	14
	Information Practices Process Development Flowchart.....	17
	APPENDIX A: CONTENT REGULATION: PRIVACY & INFORMATION MANAGEMENT — POWERPOINT SLIDES .....	19

## **I. Introduction**

The threats of identity theft and terrorism — and society's response to these threats — have galvanized our need to find workable tools for information privacy and security. Government and consumers are demanding that public and private databases be leveraged for identity verification and possible profiling of security threats, and many companies today must comply with complex requirements that they analyze and disclose personal data to the government under the USA Patriot Act and other homeland security laws. At the same time, concerns about identity theft are driving a multitude of state and federal laws, many of which seek to mandate security levels, restrict information flows and permit consumers to block access to personal data. Yet consumers continue to demand convenient access to credit and increasingly faster, more personalized customer service, all of which necessitates broad customer relationship management solutions and robust data use as well.

Informed discussions about privacy and security today must consider all of the issues related to the use of technology and information for authentication, authorization, profiling, and security. Tensions exist between the needs of privacy and as well as with the needs that companies and consumers have with respect to speed and efficiency of business transactions.

The ability to collect and use personal information is essential to our information services economy. Businesses rely on information collected from prospective and existing customers, suppliers, and government agencies to further many legitimate commercial purposes - and the ability to supplement and enhance the data with both experiential and third-party information is essential. These datasets are the infrastructure of our personalized, CRM-driven systems, and the information is used to promote business, target and improve products and services, collect debts, screen customers and employees, and prevent fraud and other crimes. These datasets are also shared with a multitude of data processors, outsourced service providers, affiliates, business partners and government agencies. However, given the proliferation of technologies which permit the storage and manipulation of vast quantities of personal data, and the ever-growing threat of identity theft, individuals, privacy advocates, and policy makers are concerned about the potential for misuse of information.

Information industry companies are generally sensitive to the value and harm generated from their products and data bases. However, many information-dependent companies struggle to understand and quantify the harms related to the actual or perceived loss of privacy or security by cus-

tomers. Privacy and security are often not even defined in a way that anticipates consumer concerns and objections. Security is objective, limiting access of information to authorized users and processes. Privacy is subjective, the use of information in ways that are appropriate, given the context.

Because privacy is subjective, even the sensitivity of the personal data collected is oftentimes not definitive. Intellectually, it is reasonable to assert that it is a greater privacy violation to reveal confidential or embarrassing information about an individual than it is to reveal publicly-known facts about the individual. However, many individuals believe that they have a privacy interest in public record information about themselves as well as in their names and addresses. In addition, the use of *any* data for targeted marketing purposes without adequate disclosure is almost always perceived as a privacy violation by individuals. Additionally, a security breach, such as inappropriate disclosure of information or an identity theft incident, is also perceived by consumers as a privacy issue. The bottom line: privacy violations are whatever individuals think they are.

## **II. Managing the Four Privacy & Security Risks**

Historically, information industry and information-dependent companies have not needed to consider the societal implications of their products. New technologies have permitted companies to increase wealth by delivering better products in a smarter, more targeted manner. However, many of these new technologies have also raised privacy and security concerns. For example, one company's attempt to build smart fraud prevention products to enable businesses to verify presenters of checks (and to deter ID theft) using photographic identification became a political and social firestorm when consumers discovered that the company was attempting to buy digitized copies of the photos on state driver's license records. Consumers and policy-makers were not persuaded that the fraud prevention potential of the product outweighed the loss of privacy that motorists would experience if their photos were available to private businesses.

There are four risks that every organization must manage around information use, and the most effective organizations manage all of these risks in a holistic manner. These risks are:

- 1. Legal Compliance** - The company must comply with all applicable laws, state, federal and international laws regarding its use of information. These include traditional privacy and data protection laws as well as new security standards and all of the laws regulating adver-

tising, government reporting, and all other laws that touch information. The company must also comply with its contractual commitments.

2. **Reputation** - The company must protect its reputation as a trusted institution with respected brands. The company must also protect all of its relationships with its non-consumer stakeholders, including its employees, independent agents, brokers or dealers, investors, vendors, regulators and business partners. The company must understand the nuances of consumer, media and government relations.
3. **Investment** - The company must receive the proper return on the investments that are made in communications and information technology, including CRM systems and other data management technology. If the company invests in businesses, products or corporate initiatives that are information-dependent, the company must understand the ROI needs for these endeavors as well. The company must understand the real revenue implications of its corporate information assets.
4. **Reticence** - The company must use information as robustly as its competitors; it must use information to retain, add and up-sell customers by delivering the right offer at the right time to the right individuals. Appropriate corporate growth, leveraging the company's informational assets, is essential to success.

Balancing these four risks requires tradeoffs to be made. One can minimize legal compliance and reputational risks by using information only in the most conservative ways, but this strategy creates too much reticence risk. If a company is meek, it leaves too much money on the proverbial table because of opportunities that are not taken. It does not provide investors or employees with appropriate growth, and it is not successful in the long term.

The same tradeoffs exist on the security side. A company can require multiple authentication steps to help ensure that it knows its customers. If these added steps increase the transaction times, however, the customer may reject the transaction in favor of a more efficient vendor. Similarly, consumers may be comfortable being asked to show a photo id to complete a credit transaction, but they may balk at a request for biometric identity confirmation, such as fingerprint. They may believe that the added security is too invasive of their privacy.

The task of finding the right balance for an organization is typically given to a chief privacy office or other privacy manager. Effective CPOs rely on a combination of good instincts and sound processes to achieve the right risk balance. For example, an effective CPO will rely on processes to ensure that proposed data uses are consistent with legal requirements and expectations. They weigh investment plans against the probability of future changed expectations. They then build consensus around the results of the processes, offering solutions that meet corporate goals in a manner consistent with the corporate culture.

### **III. A Sensible Approach to Fair Information Practices**

The secret for information industry and information-dependent companies is to develop balanced information management programs. This program serves as a framework that enables companies to achieve a variety of information policy goals ranging from development of privacy and security policies to compliance with U.S. or international data protection laws. It also provides a foundation for achieving other company goals, such as guiding marketing programs and enabling the company to anticipate business threats, the requirements of new laws, and consumer and policy-maker concerns.

Our experience shows that most companies have developed a number of privacy and security policies, but the policies are typically created in an *ad hoc* or as needed manner – for example, most companies have a “privacy policy” on their websites or a formal program to comply with the HIPAA requirements for the employee health plan. This approach solves short term problems, but does not provide the company with the holistic benefits that a formal information management program can offer.

We recommend that each organization develop a list of specific information policy objectives, then create a holistic, enterprise-wide set of business/policy standards and tools that enable the company to realize the defined objectives. This approach allows the company to generate value for the company from personal information while maintaining as much flexibility within the organization for use and distribution of data as is needed for the company to achieve both short and long term business goals. This approach also allows the company to make more informed decisions about the potential risks and returns on its investments in infrastructure technologies that facilitate communication, information management and customer relationship management. Most importantly, this approach allows the company to articulate its information policy values

and link these values to the ultimate corporate goal of building trust with company stakeholders.

By imposing a formal process approach on procedure development, companies can preserve business flexibility and maximize the success of the information management program. This approach also helps companies anticipate future changes both in the regulatory environment and in their business needs. Additionally, by considering all of the issues related to the data collected and used by the company, the company is well-positioned to leverage its program to build consumer and business partner trust. Many companies are discovering that they can gain real top and bottom-line revenue advantages by being good corporate citizens who are privacy-sensitive and who can intelligently address any questions about their information management practices.

#### **IV. Essential Elements of an Information Management Program**

Both risk management and good corporate citizenship require that organizations develop policies for the appropriate collection and use of personal information. Depending on the organization's business, these policies may include such things as maintaining opt out lists for direct marketing, developing appropriate security for customer financial or medical records, executing proper contracts to authorize international data flows, or publishing an online privacy notice if data is collected over the Internet.

Corporate privacy leaders must assist their organizations in thinking about privacy policy development in a formal, objective way, meeting policy goals as well as preserving business flexibility. Privacy executives must also understand and anticipate future changes both in the regulatory environment and in their companies' business needs. To achieve these objectives, companies should consider four distinct tasks.

##### **PHASE 1: DISCOVER**

Before you can begin to draft a privacy policy, you must first consider the company's informational goals and corporate culture. What laws regulate the company's collection or use of information? Does the company want to be able to use information as aggressively as possible? Does the company want to limit its use of information to try to achieve a competitive advantage as a privacy-sensitive leader? Does the company's executive management or shareholders have privacy issues that should be considered? How do the company's information policy objectives mesh with those of its competitors, customers and business partners? The



answers to these questions, can begin to help an organization define its core information policy goals. These goals serve as the foundation upon which the company's policies are built.

In addition to the myriad of state, federal and international laws that regulate the collection, use and/or disclosure of personal information, many industry groups have promulgated self-regulatory guidelines, some of which are mandatory for members of the specific industry group. For example, the Direct Marketing Association requires its members to comply with the provisions of the DMA's Privacy Promise. Other "mandatory" codes of fair information practices have been adopted by the Software and Information Industry Association, the Online Privacy Alliance, and the online seal providers TrustE and BBBOnline.

In the world of e-commerce, the Federal Trade Commission has been actively and aggressively pursuing companies that post privacy policies and then do not comply with their posted policy. The FTC initiates these actions under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices. Similarly, several of the state Attorneys General have initiated enforcement activities against companies that breach promises made to consumers in privacy policies. Accordingly, it is essential that, to the extent you advise your company on privacy policies, you make it clear to your management team that failure to comply with your posted privacy policies is a deceptive trade practice actionable by the FTC and other state and federal authorities.

In order to provide useful advice to your organization regarding privacy, it is essential that you understand all of the company's actual practices with regard to personal data as well as what its goals are with respect to the use of the personal data that it has collected. The success of this exercise hinges on asking the right people the right questions. The successful policy leader forges honest and open relationships with individuals in all departments and at all levels. For example, the policy leader should have regular dialogue with the individuals responsible for legal compliance, customer service, marketing, IT, and sales to determine if the company's current practices (and future goals) are clearly understood. The leader should also communicate regularly with the individuals who implement the policies and procedures to help ensure that the policies are properly adopted and that the policies address all of the questions that company personnel face.

## **PHASE 2: BUILD**

Once you understand your company's current practices and goals, you can help your company find the best way to address consumer expectations while meeting its business goals. By undertaking a formal balancing exercise, a company can realize its information policy objectives while maintaining flexibility within its organization for use and distribution of data as is needed for the company to achieve both short and long term business goals.

Additionally, by considering all of the issues related to the data collected and used by the company, the company will be well-positioned to leverage its program to build consumer and business partner trust.

## **PHASE 3: COMMUNICATE**

Once your company has developed and implemented an information management program, it is essential that you communicate the elements of the program to internal and external audiences. Internal audiences must be trained on the procedures and processes that are established, and individuals must be accountable for complying with the company's program. More importantly, the company's information policy values need to be shared with all company decision-makers and consumer-facing employees, so that they are able to use these values to shape the messages given to the company's customers and other stakeholders.

Consumer education is also critical. The primary goal of a written privacy statement is to educate consumers honestly about the actual practices of the company. The policy must accurately reflect the company's practices, and it must not mislead consumers, even by omission. A secondary goal of the privacy statement is to provide a basis for accountability of the organization with respect to its practices. We recommend that companies adopt a layered privacy notice approach - placing a template-based, standardized form privacy notice on top of a longer, more detailed statement of privacy and security practices. For a copy of the template and user's guide developed by the Center for Information Policy Leadership's Short Notices Program, please visit [www.policyleaders.com](http://www.policyleaders.com).

With regard to all privacy statements, there is a good deal of consensus as to what types of organizational practices that a privacy policy must address. At minimum, a privacy statement must include a clear notice as to what data is being collected by the organization and notice as to the intended uses and recipients of the data. Additionally, companies should inform consumers about what choices (if any) that the individual has with respect to the intended uses of the data. If the data is to be used for direct

marketing purposes or is otherwise shared with non-affiliated companies, companies are generally expected to offer individuals the ability to opt out of having the data used in these ways. Finally, the notice should include contact information for the company.

#### **PHASE 4: EVOLVE**

Finally, in order to help ensure continued compliance with the company's policies and procedures (and to help anticipate when revisions to the policies are needed), each company should initiate an ongoing education-affirmation cycle. To do this, the company would define and implement a schedule of periodic reviews of the policies, complete with employee training, and legislative monitoring (and advocacy, if appropriate). The goals of the education-affirmation cycle are to verify compliance with your company's published procedures and to position the company to proactively respond to any problematic legislative proposals and/or media events with education.

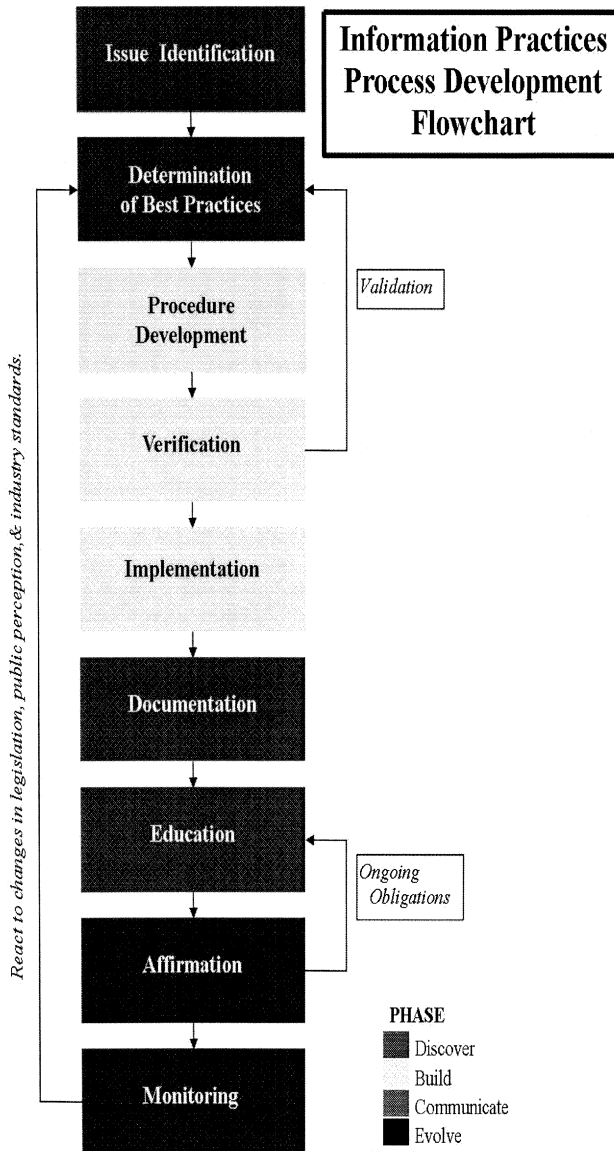
#### **V. Conclusions**

Policy leaders must assist their organizations in thinking about privacy and security policy development in a formal, objective way, striving to help the company meet policy goals as well as to preserve business flexibility. Successful policy leaders must also understand and anticipate future changes both in the regulatory environment and in their companies' business needs. In order to do this, policy leaders must be conversant in all of the business, legal, economic, social and political factors that may be relevant to the company's situation.

By imposing a formal process approach on procedure development, companies can maximize the success of the information management program because the structure of the program will permit the companies to anticipate future changes both in the regulatory environment and in their business needs. Additionally, a company can use a well-designed information policy program to develop consumer and business partner trust, and to make better investment decisions about technology infrastructure investments, resulting in top and bottom-line revenue advantages for the organization.

For more information on the Hunton & Williams privacy and information management practice solutions, the Center for Information Policy Leadership, or our Short Notices or Authentication programs, please contact Peggy Eisenhower at (404) 888-4128 or via email to *peisenhauer@hunton.com* or visit our website, *www.policyleaders.com*.

---

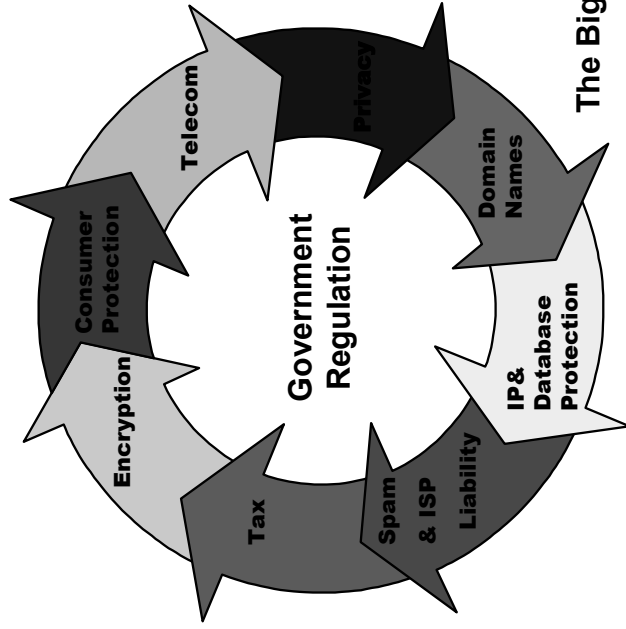


# Content Regulation: Privacy & Information Management

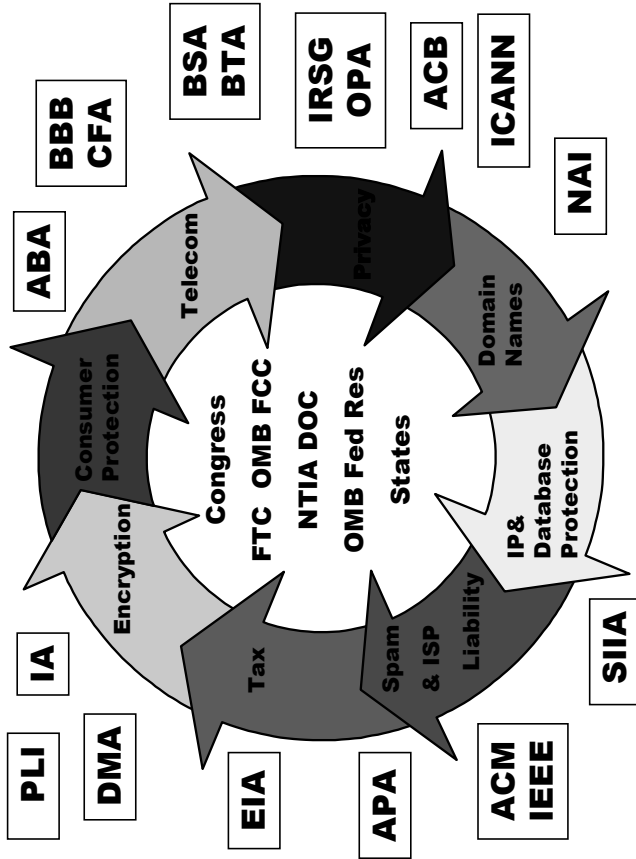
Hunton & Williams  
600 Peachtree Street  
41<sup>st</sup> Floor  
Atlanta GA 30308  
[www.hunton.com](http://www.hunton.com)

**Peggy Eisenhauer**


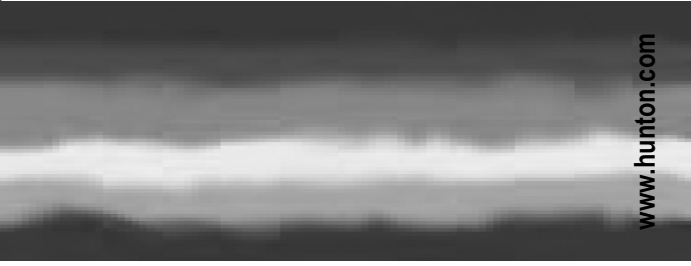
Technology, E-Commerce & Privacy Practice Group  
[peisenhauer@hunton.com](mailto:peisenhauer@hunton.com)



*But there's no consensus!*



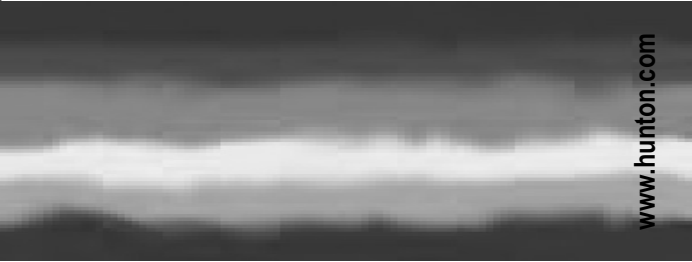


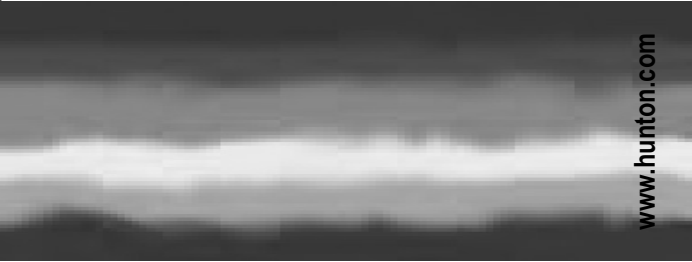
	<h2 data-bbox="242 774 284 1168">A Few Basic Truths</h2>
 <p data-bbox="945 1216 968 1416">www.hunton.com</p>	<ul style="list-style-type: none"> <li>• Collections of personal data are valuable.</li> <li>• It's very cheap to collect, store, manipulate, use and distribute data.</li> <li>• New technologies offer new uses for data.</li> <li>• There are very few disincentives to collecting and keeping data.</li> <li>• No one defines privacy, but everyone is for it.</li> <li>• People don't realize the benefits of public information.</li> <li>• Privacy violations sell newspapers.</li> <li>• It's always an election year for someone.</li> </ul>


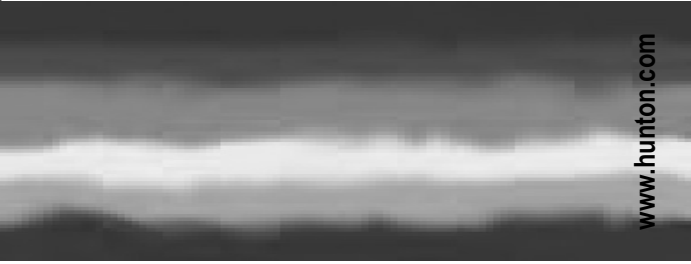
## Internet Privacy Fears

- The Internet has merged physical and informational privacy fears
- Internet privacy concerns stem from a (very real) fear of surveillance
- The nature of a transaction has shifted the balance of expectations



	
	
	<div>Legal Context Players</div>
	<ul style="list-style-type: none"><li>• Federal Trade Commission</li><li>• State Attorneys General and NAAG</li><li>• Congress</li><li>• State Legislatures</li><li>• EU, Canada and Department of Commerce</li><li>• OMB Privacy Office</li><li>• Other Federal Agencies</li><li>• Other State Policy Makers</li></ul>

	
<div data-bbox="229 300 296 1177"> <p>Business Context Players</p> </div>	<ul style="list-style-type: none"> <li>• Industry Trade Associations</li> <li>• International Trade Organizations</li> <li>• Seal Providers</li> <li>• The Fourth Estate</li> <li>• Consumer Advocates</li> <li>• Customers</li> <li>• Competitors</li> </ul>

	<h2 style="text-align: center;">The Current Regulatory Climate</h2>
 <p style="text-align: right;"><a href="http://www.hunton.com">www.hunton.com</a></p>	<ul style="list-style-type: none"> <li>• <b>Self Regulation</b> - OPA, DMA, BBBOonline, TrustE</li> <li>• <b>Existing and New Federal Laws</b> <ul style="list-style-type: none"> <li>- Use Restrictions (FCRA, DPPA)</li> <li>- Collection and Access Restrictions (COPPA)</li> <li>- Notice Requirements (GLB &amp; Reg P)</li> </ul> </li> <li>• <b>State Initiatives</b> - CA, NY, GLB counterparts</li> <li>• <b>International Data Protection Laws</b> <ul style="list-style-type: none"> <li>- EU and Safe Harbor</li> <li>- Canada, Hong Kong, Etc.</li> </ul> </li> </ul>

**Also be aware of state and federal Unfair  
and Deceptive Trade Practices  
Statutes...**

**You gotta walk your talk!**



	 <a href="http://www.hunton.com">www.hunton.com</a>
<div data-bbox="230 302 296 1178"> Privacy Issue Spotting Opportunities </div>	<ul style="list-style-type: none"> <li>• Development of privacy policies, web site Ts &amp; Cs, evaluation of seals, self-regulatory schemes</li> <li>• Development of new products, expansion into new markets, channels, geographies</li> <li>• Development of advertising materials and promotional campaigns</li> <li>• Preparation of marketing, data sharing, promotional, e-commerce, outsourcing agreements</li> <li>• Resolution of consumer complaints, litigation, enforcement authority investigations</li> <li>• M&amp;A due diligence, VC and securities disclosures</li> </ul>

## The Business Reality

- Privacy issues can arise in every type of technology project or transaction. And privacy issues affect online and offline data stores.
- In order to effectively address privacy issues, the company must understand both the legal and business contexts.
- Legal compliance is essential, but the business context should determine each company's privacy values and, ultimately, its privacy policies.



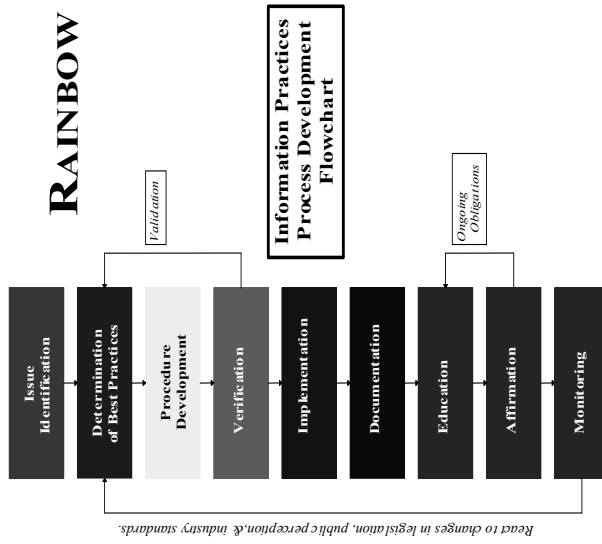
	<div data-bbox="230 302 296 1177">Privacy Policy Thought Leaders</div>
 <div data-bbox="944 1216 971 1416">www.hunton.com</div>	<ul style="list-style-type: none"> <li>• Provide traditional legal advice regarding compliance with laws, advocacy</li> <li>• Provide business advice regarding best practices, business risks and benefits</li> <li>• Craft enterprise-wide solutions that meet consumer and policy expectations while providing the company with appropriate data flow opportunities</li> <li>• Find the right balance for the company, given the company's culture and corporate goals</li> </ul>

## Developing Enterprise-Wide Programs

- Consider your corporate culture
- Understand your organization's data collection and sharing practices - and make sure that everyone else understands them too
- Brainstorm about long term data, technology and product goals; anticipate outsourcing relationships, new products, channels, customers, geographic markets
- Analyze industry practices, regulatory climate, then evaluate legal and business risks and advantages


	<h2 style="text-align: center;">Developing Enterprise-Wide Programs</h2>
 <p style="text-align: right;"><a href="http://www.hunton.com">www.hunton.com</a></p>	<ul style="list-style-type: none"> <li>• Formalize implementation controls, testing, documentation</li> <li>• Draft <i>consumer-oriented</i> privacy policies that <i>educate</i> in plain English and that serve as business and marketing tools (for customers, investors and other stakeholders)</li> <li>• Establish an “affirmation-education cycle” to monitor law and media for needed adjustments</li> </ul>


## The H&W Approach: RAINBOW




*React to changes in legislation, public perception, & industry standards.*


	<p><b>RAINBOW:</b> <i>an approach to fair information practices</i></p>
 <p><a href="http://www.hunton.com">www.hunton.com</a></p>	<ul style="list-style-type: none"> <li>• A 7-step facilitated self-assessment process to meet policy, legal and business goals - legal compliance, licensing, advocacy, marketing, sales and public relations</li> <li>• Supports enterprise-wide planning with a focus on business flexibility – policy &amp; procedure development designed around company needs and industry best practices</li> <li>• Includes a comprehensive examination of the organization's data flows, compliance mechanisms, and provides implementation and documentation guidance</li> </ul>


	<div>Issue Identification</div>
<div> <div>RAINBOW</div> <div>Step 1</div> </div> <div>www.hunton.com</div>	<div> <div>Goals:</div> <ul style="list-style-type: none"> <li>• Develop baseline knowledge of current practices</li> <li>• Understand current &amp; future business goals</li> <li>• Identify potential conflicts between legal requirements, business needs &amp; policy goals</li> <li>• Educate management on legal and policy concerns</li> <li>• Establish priorities</li> </ul> <div>Activities:</div> <ul style="list-style-type: none"> <li>• Explore current company information practices</li> <li>• Investigate customer and consumer concerns</li> <li>• Analyze the legal context as it relates to your business</li> <li>• Relate legal, policy and public relations issues to current and planned practices</li> <li>• Evaluate short and long term business needs and goals</li> </ul> </div>


	<div>Determination of Best Practices</div> <div><p><b>Goals:</b></p><ul style="list-style-type: none"><li>• Educate company employees and partners on perceived best practices</li><li>• Identify ways to balance business needs and goals with legal and policy needs and goals</li><li>• Develop consensus on company approach to information management and privacy issues</li></ul><p><b>Activities:</b></p><ul style="list-style-type: none"><li>• Examine industry standard practices</li><li>• Review current regulatory environment</li><li>• Analyze existing industry self-regulatory regimes</li><li>• Anticipate future legal, policy and consumer issues as well as other stakeholder issues (suppliers, investors)</li></ul></div>
<p><b>RAINBOW Step 2</b></p> <p><a href="http://www.hunton.com">www.hunton.com</a></p>	


	<div>Procedure Development</div>
<div>RAINBOW Step 3</div> <div>www.hunton.com</div>	<div>Goals:</div> <ul style="list-style-type: none"> <li>• Structure specific procedures that permit beneficial uses of information while complying with applicable laws</li> <li>• Develop procedure generation and review process that can accommodate new products, business expansion and the changing regulatory climate</li> </ul> <div>Activities:</div> <ul style="list-style-type: none"> <li>• Define company-specific information management procedures covering data collection, access, use and distribution</li> <li>• Identify appropriate quality assurance standards and measures</li> <li>• Devise appropriate legal compliance, consumer affairs and policy advocacy initiatives</li> </ul>



	
<b>RAINBOW Step 4</b>	<div>Verification</div> <p><b>Goals:</b></p> <ul style="list-style-type: none"><li>• Confirm that the procedures will achieve the desired results and that all business and legal needs and goals are addressed by the procedures</li><li>• Confirm that implementation of procedures will not result in unanticipated hardship or loss of flexibility</li><li>• Confirm that company's practices are comprehensively covered by the procedures</li></ul> <p><b>Activities:</b></p> <ul style="list-style-type: none"><li>• Validate conformity between defined procedures and policy goals</li><li>• Identify any gaps between new procedures and actual company practices</li><li>• Confirm that all business and legal needs, goals are met</li><li>• Vet procedures against industry best practices</li></ul> <p><a href="http://www.hunton.com">www.hunton.com</a></p>


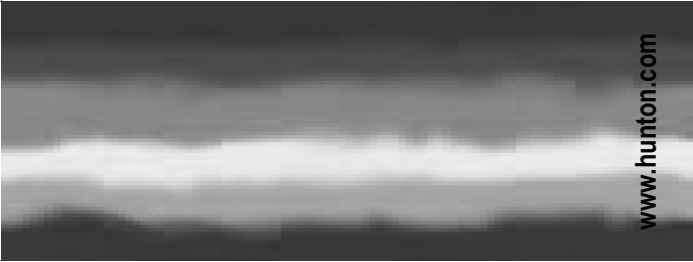
	<div>Implementation</div>
<div> <div>RAINBOW</div> <div>Step 5</div> <div>www.hunton.com</div> </div>	<div> <div>Goals:</div> <ul style="list-style-type: none"> <li>• Become fully compliant with established procedures</li> <li>• Help ensure ongoing compliance through accountability</li> </ul> <div>Activities:</div> <ul style="list-style-type: none"> <li>• Initiate full compliance activities in accordance with the procedures; Designate accountable individuals</li> <li>• Begin maintaining access logs and audit trails, institute appropriate security mechanisms for facilities, computers</li> <li>• Develop and execute employee and contractor agreements, confidentiality and access agreements (as needed)</li> <li>• Develop and distribute educational materials for employees, contractors, affiliates, others; conduct employee training</li> <li>• Launch consumer affairs program, initiate advocacy, public relations programs as appropriate</li> </ul> </div>

	<div>Documentation</div> <div><p><b>Goals:</b></p><ul style="list-style-type: none"><li>• Establish roles, responsibilities and communication channels</li><li>• Create formal written records of procedures, policy objectives, accountable parties and implementation details</li><li>• Develop records to support compliance status reviews</li></ul><p><b>Activities:</b></p><ul style="list-style-type: none"><li>• Document all compliance steps</li><li>• Define and document clear roles and responsibility for ongoing compliance and program oversight; assign responsibility for documentation maintenance</li><li>• Draft written privacy policy, customer notices<ul style="list-style-type: none"><li>– Goal is consumer education - <i>marketing, stakeholder relations</i>.</li><li>– Must be accurate!</li><li>– Must address five essential elements:<ul style="list-style-type: none"><li>Notice, Choice, Access, Data Integrity, Security</li></ul></li></ul></li></ul></div>
<p><b>RAINBOW Step 6</b></p> <p><a href="http://www.hunton.com">www.hunton.com</a></p>	

	<div data-bbox="230 298 296 1177"> <h1>The Education-Affirmation Cycle</h1> </div>
<div data-bbox="357 1241 456 1399"> <h2>RAINBOW Step 7</h2> </div> <div data-bbox="944 1216 971 1414"> <a href="http://www.hunton.com">www.hunton.com</a> </div>	<div data-bbox="334 1067 365 1164"> <h3>Goals:</h3> </div> <ul data-bbox="382 315 565 1164" style="list-style-type: none"> <li>• Ensure continued compliance with procedures by ongoing monitoring and education activities</li> <li>• Proactively respond to any legislative proposals or media events with education, policy-shaping suggestions, advocacy</li> <li>• Reap public relations benefits from your compliance efforts</li> </ul> <div data-bbox="600 1013 631 1164"> <h3>Activities:</h3> </div> <ul data-bbox="648 324 944 1164" style="list-style-type: none"> <li>• Establish schedule and process for periodic review of procedures and verification that procedures are being followed</li> <li>• Establish schedule and process for employee training, other training for new hires, new suppliers, new customers, new business partners</li> <li>• Continue legislative and media monitoring, lobbying and advocacy activities as needed and appropriate</li> <li>• Participate in external education and policy activities; commence public relations campaign activities, media analyst outreach</li> </ul>

	<div data-bbox="239 940 287 1170">The Future</div>
 <div data-bbox="945 1216 968 1416">www.hunton.com</div>	<p>Privacy sensitivity is evolving, and the expectations of consumers, customers, suppliers, policy makers and regulators can change rapidly. Each company can maximize flexibility and minimize costs by anticipating the privacy and data flow issues that may arise in all aspects of its business.</p>

	<div data-bbox="230 300 296 1177"> <h2>Our Response</h2> </div>
	<p>In order to effectively address privacy issues, companies must understand both the legal and business contexts.</p> <p>A formal process management system provides a useful framework for anticipating and addressing privacy issues in a manner consistent with the company's business objectives and core information policy values. This framework can help ensure the continued success of the company's fair information practices programs.</p>

	 <a href="http://www.hunton.com">www.hunton.com</a>
<p>For More Information</p>	

**Please contact the Hunton & Williams  
Technology, E-Commerce & Practice Group:**

Margaret P. Eisenhauer, Esq.  
Direct: (404) 888-4128  
[peisenhauer@hunton.com](mailto:peisenhauer@hunton.com)

Oscar Marquis, Esq.  
Direct: (404) 888-4277  
[omarquis@hunton.com](mailto:omarquis@hunton.com)

Scott Hobby, Esq.  
Direct: (404) 888-4263  
[shobby@hunton.com](mailto:shobby@hunton.com)

HUNTON &  
WILLIAMS

Questions?

[www.hunton.com](http://www.hunton.com)