HBR CONSULTING

The United States Culture of Privacy

Laurie Fischer, CRM, CIPT
Managing Director, HBR Consulting
lfischer@hbrconsulting.com
November 12, 2019

ARMA CHICAGO

Session Topics

- **United States Privacy Environment**
- **Privacy Everywhere Else**
  - **Why the Difference?**
- **Today's Sense of Urgency**
- **Creating a Culture of Privacy**

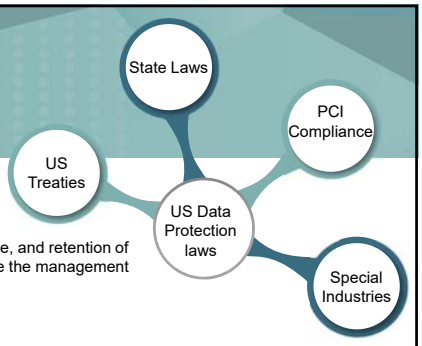
Privacy Across the Globe

U.S. Privacy Overview

- The word “privacy” does not appear in the Constitution
- Inferred by legal scholars using elements of the Bill of Rights, such as the Fourth Amendment
  - Bans unreasonable search and seizure
- No single, comprehensive federal law regulating the collection and use of personal data
- Patchwork of federal laws regulating specific sectors
- Fifty state (mostly reactive) regulations

HBR CONSULTING

United States and Privacy



OVERVIEW

Unlike many countries, the United States does not have one "Data Protection Law" intended to limit the collection, use, and retention of the personal data of individuals. Instead, the United States has the following set of laws and regulations that regulate the management of personal data:

US Treaties

Privacy Shield - Designed by the U.S. Department of Commerce and the European Commission, The Privacy Shield provides companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

Non-Governmental Agreements

Payment Credit Card Industry ("PCI") Standards works with merchants and business that use and process credit card information. PCI Standards set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

State Laws

Currently all 50 States, plus the District of Columbia, have enacted some form of privacy legislation. These are primarily reactive laws, addressing notification requirements associated with breaches of personal and protected information. A few states have recently enacted laws that give consumers rights to control or limit the information companies may retain or use.

Special Industries

Certain industries have data protection laws. Examples of these include privacy requirements for banking and financial institutions, organizations marketing to children, healthcare, and insurance companies. As a general rule, unfair and deceptive trade practices can apply to any organization that fails to comply with their own posted data privacy policies.

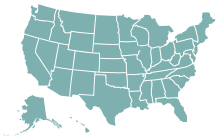
Federal Regulations

- Federal Trade Commission Act (15 U.S.C. §§41-58) (**FTC Act**) is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies.
- Financial Services Modernization Act (Gramm-Leach-Bliley Act (**GLBA**) (15 U.S.C. §§6801-6827) regulates the collection, use and disclosure of financial information. It can apply broadly to financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products.
- Health Insurance Portability and Accountability Act (**HIPAA**) (42 U.S.C. §1301 et seq.) regulates medical information.
- The Children's Online Privacy Protection Act **(COPPA)** aims to protect privacy of children under 13 years of age, specifically from the collection of their personal information online.

Federal Regulations (cont.)

- Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) which amended the Fair Credit Reporting Act) applies to consumer reporting agencies, those who use consumer reports (such as a lender) and those who provide consumer-reporting information (such as a credit card company).
- Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030)
- Family Educational Rights and Privacy Act (**FERPA**) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.
- Payment Card Industry Data Security Standard (**PCI DSS**) is an information security standard for organizations that handle branded credit cards.

U.S State Privacy Regulation



- States (and even cities) are increasingly passing laws to protect state / city residents. Since the GDPR effective date:
  - Iowa has enacted a state law that applies to operators of online services directed at and used by students in kindergarten through grade 12
  - Nebraska has passed a law that applies to all commercial entities doing business in Nebraska who own or license Nebraska residents' personal information
  - Vermont passed the country's first law regulating data brokers, which are essentially companies that sell people's information
  - Chicago City Council introduced the Personal Data Collection and Protection Ordinance that closely mirrors the GDPR requirements.

HBR CONSULTING

Other State Responses

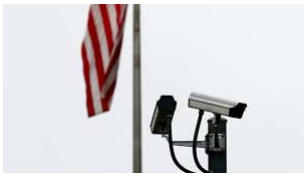
State	Action
Alabama	Finally adopted a data breach law
Arizona	New personal data protection definition, and defined notification timeline
Colorado	Requirement of security policies; oversight of third parties
Iowa	Added securities to protect children online
Louisiana	Requires organizations to take reasonable steps to destroy records with personal information that the business does not intend to retain
Nebraska	Requirement of security policies; oversight of third parties
Oregon	Tighten data breach notification laws
South Carolina	New data protection laws in the insurance industry
South Dakota	Finally adopted a data breach law
Vermont	Regulation of "data brokers," which also includes registration fee ($100)
Virginia	New requirements for those who prepare income tax returns

And then there is the CCPA…

Under the new law, California residents will have a right to:

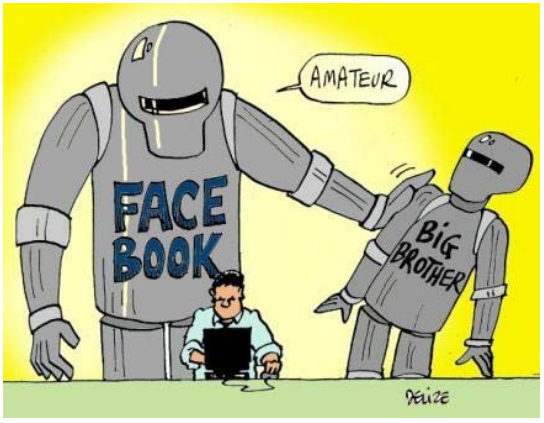
- Know what personal information is being collected about them
- Access that information
- Know if their personal information is shared, and with whom
- Know if their personal information is sold and be given the right to opt out of the sale
- Receive equal service and price whether or not they exercise their privacy rights
- Sue under a private right of action for data breach with statutory penalties substituted for actual damages

American view of privacy



- Privacy is important
- Pervasive sense they are under surveillance
- Few feel they have a great deal of control
- Low confidence in the privacy and security of records maintained by a variety of institutions in this digital age – including social media sites utilities, phone companies, government, search engines, etc. (75%)
  - Slightly higher confidence level in credit card companies
- Want to be able to share confidential matters with another trusted person
- Want online sites, search engines and social media to NOT retain any records of their history
- While 70% use social media 90% say they have lost control of their personal information

Despite the survey results…



…few have changed their behavior*

* Only 7%

Change is on the way

Digital Behavior

- **Naiveté phase**, where consumers didn't really understand the technology and what it meant
- **Careless phase**, where people saw data rights or privacy as either unimportant or an acceptable price of entry to all the good, free stuff
- **Demand phase**, which sees the emergence of a more savvy, engaged, and alarmed digital consumer — and related movements to create and enforce consumer rights

Privacy Elsewhere

- Privacy is a universal human right
- European survey respondents overwhelmingly value their privacy
- 71 percent of respondents rejected the notion of companies sharing information about them without their permission
  - It didn't matter if companies used that information to develop new services they might like. Their privacy mattered more to them.
- Data should not be kept simply because storage is cheap
- Data should not be processed simply because algorithms are refined
- Safeguards should apply and citizens should have rights

Data Protection / Privacy Laws

- Regulators understand the need to build trust in order to avoid withdrawal from the benefits of digital economy, thus strict data protection laws

GDPR

- *"There's so much misinformation out there. I want to be clear that this law is not about fines. It's about putting the consumer and citizen first…. The fine is really a last resort….On the one hand, it has certainly "got the attention of the C-Suite," On the other hand, though, it has given rise to a cottage industry of FUD [fear, uncertainty and doubt] purveyors, vested interests and mischief makers."*
  - *Elizabeth Denham, UK ICO Commissioner*

In the E.U.

- Personal information cannot be collected without consumers' permission, and they have the right to review the data and correct inaccuracies
- Companies that process data must register their activities with the government
- Employers cannot read workers' private e-mail
- Personal information cannot be shared by companies or across borders without express permission from the data subject
- Checkout clerks cannot ask for shoppers' phone numbers

Why the difference?

- Basic divergence in attitude
  - Europeans reserve their deepest distrust for corporations
  - Americans are far more concerned about the government invading their privacy
  - In Europe the first line of defense against private wrongdoing is the state
  - In the U.S. let private actors sue each other
- Example:
  - A French court ruled that Nikon France could not fire an employee for performing freelance work on the job because the incriminating e-mails were marked "personal," and thus could not be used as grounds for dismissal
  - In the U.S., employees surrender most of their rights to privacy when they enter and use company property

History + the GDPR

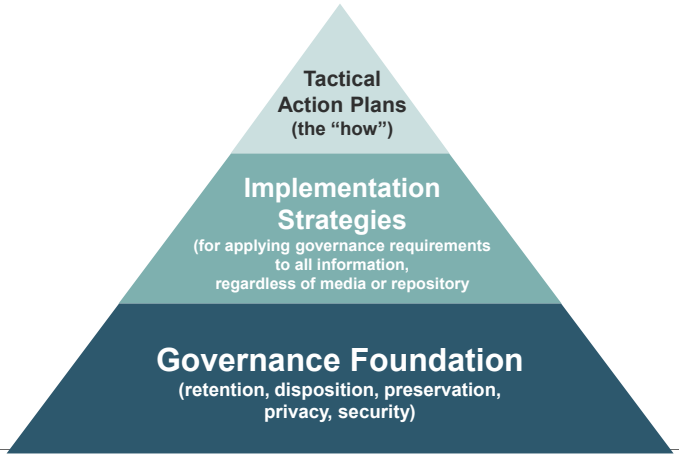
History

- Heightened European sensitivity to privacy may stem from the horror of the Holocaust, when the Nazis used public and church records to identify Jews to be rounded up and sent to concentration camps
  - In 1930s Germany, census workers went door to door filling out punch cards that indicated residents' nationalities, native language, religion and profession
- As the Nazi regime rose to power, state control of businesses brought with it state control of information technology
- In the occupied Netherlands, the Nazis exploited official registers of Dutch citizens in order to identify Jews for deportation to death camps

A different perspective on the GDPR

- Best thing that ever happened to the Information Governance professional??
  - Maximum versus minimum retention times
  - No more “just in case” or “culture of keep”
- Goal of defensible disposition to reduce:
  - Unnecessary e-discovery costs
    - Over-collection and production
  - **Greater likelihood of sensitive data breach**
  - Inability to find and retrieve needed information
  - Data duplication and redundancy
- Fines are real

Defensible Disposition is dependent on a clear definition of legal, regulatory, privacy and operating requirements



A Culture of Privacy

Creating a culture of privacy

- Build a cross-functional team – privacy, compliance, legal, IT security, business functions retaining private information
- Know where you stand today
  - Privacy risk analysis
    - Policies, practices, roles, responsibilities, accountabilities, training, technologies
      - Regulatory environment
  - Security often assumed to be the realm of IT only
    - Employee is often the “single point of failure”
  - Data mapping – where is the most sensitive data?
    - Finance, HR, Marketing, Sales, Customer Service, etc.

Critical Success Factors

- Executive team buy-in and active engagement – “Tone at the Top”
- Create a sense of urgency
  - Direct relationship between the organization’s ability to deliver and a strong privacy culture
- Create value – how does this contribute to the bottom line
- Align the message to your mission and vision, your values and guiding principles
- Real-life examples of damage to brand, reputation and bottom line
- Visible and continuous support by the C-suite

Integrate Privacy into Current Business Process

- New employee orientation
- Code of Conduct
- Annual security / privacy training
- Build “privacy by design” into new system development process
  - Privacy Impact Assessment criteria
- RFI / RFP Process / Third Party Contracts
- Risk Management – how does this impact the company’s risk profile reported to the Board
- Incident management teams – how to leverage that for your own privacy breach procedures and protocols

Change Management: Prepare

- Understand your culture of change
  - What has worked in the past?
- Define roles, responsibilities, accountabilities
  - Sponsors
  - Change champions
- Develop / Update Policies and Procedures
  - Data Classification / Handling requirements
- Understand background technology

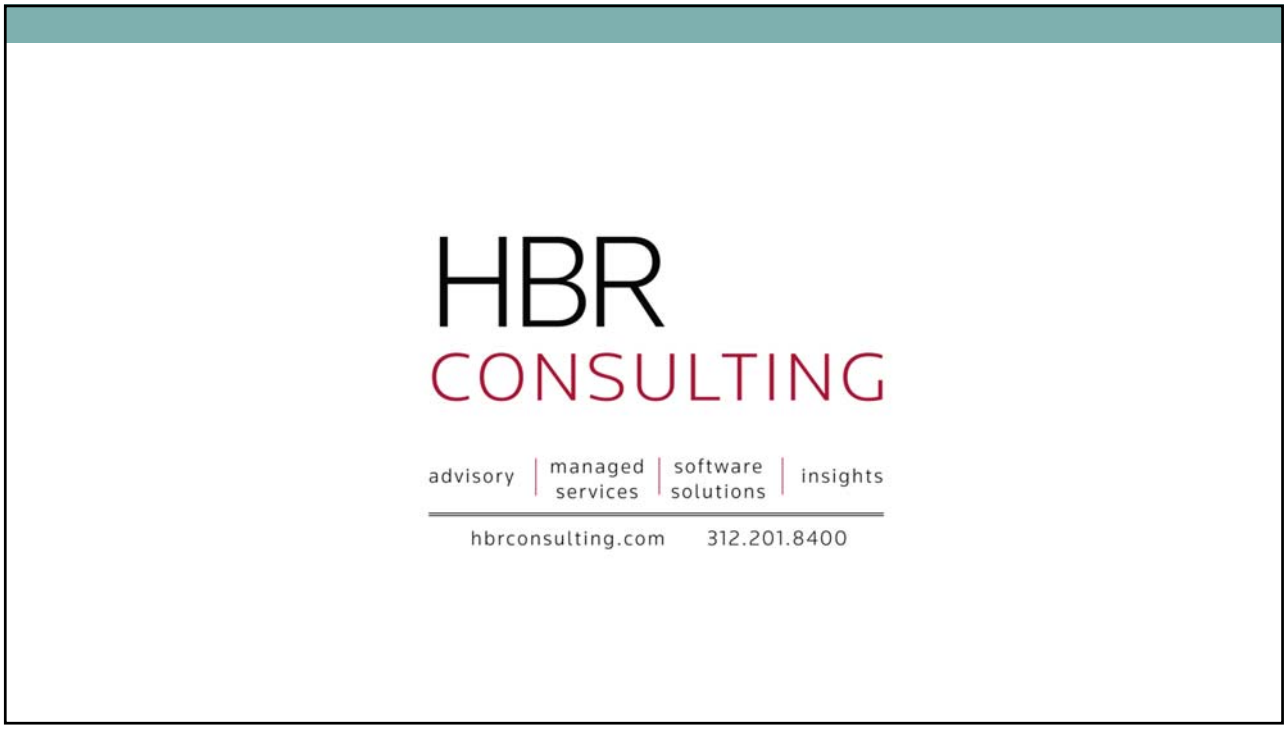
Change Management: Enact

- Privacy Awareness Campaign
- Develop Key Messages
  - Highly visible, consistent and engaging communications
  - Relatable, real-life experiences
  - “If you collect it, protect it”
- Multimedia and multi-channel communications
  - Partner with learning and development, communications and HR
- Training
- Links to training and news stories
- Relatable, real-life experiences

Change Management: On-going

- Goal: Embed privacy into the culture of the organization
- Periodic campaigns
- Executive messaging
- Role of Internal Audit and Compliance
- Measure / Metrics

Comments / Questions?


HBR
CONSULTING
advisory
managed services
software solutions
insights
hbrconsulting.com
312.201.8400