# PRIVACY PRINCIPLES – AN INTERACTIVE DISCUSSION

MARY BETH HAMES, IGP

ARMA SW REGION DIRECTOR

FEBRUARY 2020

# PRIVACY MATTERS….


**Equifax:$700M** **MyFitnessPal: $150M**

**Facebook:$29M** **Cambridge Analytica $87M**

**Saks:$5M** **T-Mobile: $2M**

# SURPRISING KEY COMPONENT OF PRIVACY

- Companies historically were focused on the risk of losing data than on retaining too much data. Understandably, they saw the significant penalties for **failing to** either:
  - retain the documents they were obligated to retain by statute;
  - take reasonable steps to preserve information reasonably relevant to potential litigation or investigation.
- Companies may have understood that there were costs to over-retention, such as increased discovery costs, but these seemed to pale in comparison to the sanctions for failing to retain what you had to keep.

# PRIVACY AND SECURITY – WHAT'S THE DIFFERENCE?

While security and privacy are interdependent, security **can be achieved without privacy, but privacy cannot be achieved without security**. Security protects confidentiality, integrity and availability of information, whereas privacy is more granular about privacy rights with respect to personal information.

- Information privacy - Wikipedia


Mac
iPad
iPhone
Watch
TV
Music
Support
Privacy
Overview
Features
Control
Transparency Report
Privacy Policy
Privacy
Privacy is a fundamental human right. At Apple, it's also one of our core values. Your devices are important to so many parts of your life. What you share from those experiences, and who you share it with, should be up to you. We design Apple products to protect your privacy and give you control over your information. It's not always easy. But that's the kind of innovation we believe in.

# WHY PRIVACY MATTERS

- *Increased regulation and enforcement action puts a new focus on personal information*
- Privacy issues continue to make their way into mainstream media coverage with huge fines (Marriott & FB) and other horror stories
- Average cost of breach $3.62 Million or more

# WHY PRIVACY?

- Privacy isn't just an IT security posture
- Strong privacy programs provide a structure for compliance, management, and audit criteria
- Should be an integral part of your corporate DNA
- Helps define your brand, determine your customer relationships and may ultimately drive your bottom line

# WHAT IS A "PERSONAL DATA BREACH"?

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" - CCPA

# WHERE'S THE RISK?

- Damage to the organization's reputation, brand, or business relationships
- Legal liability and industry or regulatory sanctions & fines
- Charges of deceptive business practices
- Customer or employee distrust
- Denial of consent by individuals to have their personal information used for business purposes
- Lost business and consequential reduction in revenue and market share
- Disruption of business operations
- Liability resulting from identity theft

# GAPP PRIVACY: WHAT ARE THE GENERALLY ACCEPTED PRIVACY PRINCIPLES?

Recognizing the challenges that businesses face in addressing privacy risks, the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) organized the Privacy Task Force to create a comprehensive framework that organizations could use to effectively manage their privacy risks. The Privacy Task Force considered international regulatory privacy requirements and industry best practices to develop the privacy guidance. The framework developed by the Privacy Task Force is called the Generally Accepted Privacy Principles (GAPP). The GAPP consists of ten privacy principles.

# WHAT QUALIFIES AS PII?

- Name, address, phone number, email address
- Social security number, driver's license number, etc.
- Biometric information –
- Certificate/license numbers
- Vehicle Identifiers
- Internet or other electronic network activity information, including, but not limited to: browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- Geolocation data
- Audio, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information
- Education information, defined as information that is not publicly available
- Inferences drawn from any of the above examples that can create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

# WHAT ARE THE PRINCIPLES

- **Management.** The entity ***defines, documents, communicates, and assigns accountability*** for its privacy policies and procedures. (see ARMA Policy Template)
- **Notice.** The entity ***provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed***.
- **Choice and consent.** The entity ***describes the choices available to the individual and obtains implicit or explicit consent*** with respect to the collection, use, and disclosure of personal information.
- **Collection.** The entity ***collects personal information only for the purposes identified*** in the notice.
- **Use, retention, and disposal.** The ***entity limits the use of personal information*** to the purposes identified in the notice and ***for which the individual has provided implicit or explicit consent***. The entity ***retains personal information for only as long as necessary*** to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
- **Access.** The entity ***provides individuals with access*** to their personal information for review and update.
- **Disclosure to third parties.** The entity ***discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.***
- **Security for privacy.** The entity ***protects personal information against unauthorized access*** (both physical and logical).
- **Quality.** The entity ***maintains accurate, complete, and relevant personal information*** for the purposes identified in the notice.
- **Monitoring and enforcement.** The entity ***monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes***.

# CREATING AN ASSESSMENT AND ROADMAP

- Create a strategy or vision for the organization's long-term direction and prosperity helps define the culture and helps shape how the it will interact with external entities, including its customers. This process should also help develop an overall master plan based on its strategic direction. Having a clear strategy and master plan should help clarify the objective and align the organization toward it. If privacy compliance is a critical component to your organization's success, your strategic plan should identify the long-term goals and major obstacles for becoming compliant with relevant privacy laws and regulations.
- With long-term goals established, the final step of strategizing is assigning resources to execute the plan. The allocation of resources would include the identification and assignment of human, financial, and other resources for the strategic plan.

# ASSESSMENT PHASE - PRIVACY MATURITY ASSESSMENT AND ROADMAP

- Privacy Data identification
- Privacy assessment
- Gap Analysis & remediation
- Resource requirements
- Strategic planning

# ASSESSMENT PHASE - PERSONAL INFORMATION INVENTORY

- Data flow analysis
- Inventory of PII data repositories
- Creation of a Master Data Inventory (Data Map)

# FOUNDATION – PRIVACY POLICY & PROCEDURES

- Policy development
- Privacy Notice development
- Consent documentation
- Procedures development
- Supply Chain/3rd party clause development

# FOUNDATION – DATA SECURITY & PRIVACY CONTROLS

- Data security classification review/refresh
- Privacy data controls & safeguards
- Breach Response Plan

# IMPLEMENTATION – PRIVACY DATA & INFO GOV

- File plan development
- Taxonomy development
- Information rights
- Data migration

# IMPLEMENTATION – ACCESS REQUEST & TRACKING

- Request tracking process development
- Authentication process development
- Search process development
- Production process development
- Deletion process development

# IMPLEMENTATION – PRIVACY COMMUNICATION & TRAINING

- Communication & training plan dev
- Employee training
- Consumer training
- Training delivery

# IMPLEMENTATION – LEGACY DATA REMEDIATION

- Unstructured data
- Back up tape
- Email
- On & offsite hard copy inventory

# PRIVACY'S TIME HAS COME – 12 BEST PRACTICES

# WHAT SHOULD I DO NEXT?

- Make the case for Privacy to senior management
- Get key stakeholders on board
- Design, implement and communicate privacy policy
- Establish and manage privacy programs
- Monitor and audit privacy programs
- Measure performance and benchmarking

# AVOIDING THE PITFALLS

- **"Policy-itis"** A common roadblock to privacy programs – focusing on the development of a privacy policy to the exclusion of policy execution. Compliance is achieved not just through having a policy, but also by faithfully implementing it as well.
- **Siloed approaches** Effective privacy takes **a team,** including privacy, legal, compliance, IT and business units
- **Manual or unworkable processes** Manually compiling personal information access and deletion requests is likely to become overwhelming. Organizations need to consider making this an automated, streamlined approach.
- **It's never too late to start -** CCPA enforcement began on January 1, 2020. Organizations that start creating their programs too late run the risk of not completing on time.

# IN CLOSING…..

- Don’t let the perfect be the enemy of the good
- Privacy is an incremental process which will help reduce risk over time
- Build your privacy skills and your career!

# RESOURCES

- ISO27701 – Privacy Add-on Assessment
- Privacy Terms - https://iapp.org/resources/glossary/
- Google University
- https://www.ftc.gov/tips-advice/business-center/privacy-and-security/consumer-privacy
- https://iapp.org

Mary Beth Hames, IGP

SW Region Director at ARMA

InfoSec Compliance Analyst @ PNM (Electric Utility)

Marybeth.hames@pnmresources.com

hamesmb@gmail.com

505-448-6710