IAPP KnowledgeNet – San Francisco Bay Area Chapter

June 19, 2018; 8:30 – 11:30 am PDT

Symantec Corporation

350 Ellis Street, Mountain View, CA 94043

"OUR JOURNEY CONTINUES – Building & Sustaining a Robust Global Privacy Program"

Panel 1: Privacy Operating Models

Panel 2: Operationalizing Global Privacy & GDPR Requirements

Key Learnings*

PANEL 1: Privacy Operating Models

1. Who should own privacy in the organization

- It depends on the organization's structure, risks, resources, and individuals
- Privacy could be in Legal, Compliance, or Information Security
- Privacy needs both legal and operationalization capabilities
- Most successful Privacy ownership and roles seem to be under Legal and Compliance
- Legal focuses on law and interpretation, Compliance on operationalization
- Many organizations have Privacy owned by Compliance
- HR and IT are often involved, but do not necessarily have ownership
- HR and IT may not be neutral ("fox watching henhouse"), and may have other priorities
- The recent trend is to have Privacy owned by Compliance
- Ownership by Legal in smaller organizations makes the most sense
- Privacy and Security groups often roll up to the general counsel
- A separate Privacy Office could be under the IT umbrella

2. Governance and structure -- what works and doesn't, and what are success factors

- Needs a cross-functional governance model
- Privacy is often led by a Privacy Officer who has executive sponsorship and visibility at the board level
- Privacy Officers are getting more responsibility
- Regional and business representation is very important
- Attract and involve board members showing interest in Privacy; orchestrate executive learning sessions
- GDPR forced organizations to look closely at governance structure
- Bring in Privacy reps and champions ("knights of the roundtable") from business units and functions
- Privacy champions, ambassadors, and "knights of the roundtable" can be an effective recruiting tool
- GDPR is a great stick that bolsters governance and compliance
- Get support from Finance and IT to fund compliance, tools, and tech applications costs
- Know where personal data is located within the organization and with third-party vendors/partners
- Cultural values matter a lot in corporate governance matters

3. What kind of models work best -- centralized, decentralized, hybrid

- A “centralized” Privacy program means having a central Privacy Office with fulltime Privacy staff
- A “decentralized” structure means Privacy staff is spread throughout the globe, with region personnel doing their own thing
- Most organizations have hybrid or centralized models, with reps in different geographies
- A “Management Review Committee” can address difficult issues and make decisions
- Consider specific or additional Privacy requirements in different geographies
- Identify revenue streams and identify key stakeholders from regions/countries driving the most revenue
- Reading between the lines of business and Privacy key performance indicators (KPIs) is crucial
- Look at governance models through a worldwide lens
- Important to hear from people close to the customers, to really understand customer needs
- Many European customers demand onsite audits
- Embed Privacy in an organization’s culture and human capital change management process
- Ensure people are sufficiently engaged, especially in large organizations
- Use incentives to attract employees interested in Privacy-related roles and initiatives

4. What capabilities do we need -- privacy by design, vendor management, tools, etc.

- Many Privacy laws and regulations are at high level
- Need to understand, operationalize, and sustain requirements across all geographies
- Need adequate budget, resources, and Privacy personnel with the right skillsets
- Require ability to take Privacy requirements to a program level and rolling them out to geographies
- Need effective management of global supplier risks and understanding of contractual requirements
- Need sensitivity and appreciation of the global nature of Privacy (“global fluency”)
- Be open to disparate ideas and applying them as appropriate, without tribal or institutional bias
- Embedding Privacy by Design (PbD) in products is becoming a norm for organizations
- Building and rolling out Privacy-enabled products globally is a huge undertaking
- Many organizations respond better to the GAPP/AICPA maturity model, as compared to risk-based models
- A maturity model helps governance committees focus on what maturity level to aim for
- Internal audit or business management tends to respond better to a maturity model
- A maturity model is getting increasingly popular with many organizations
- To address complexity and facilitate corporate change, create relevant documentation and training programs

5. Industry-leading practices and trends

- A code of ethics should have Privacy components weaved in
- Use of tools and automation for personal data recordkeeping is increasing
- Adequate data and process granularity is necessary for obtaining actionable Privacy insights
- Privacy Impact Assessment (PIA) tools are very useful for assessing business and geographic risks
- Whistleblower protection has become a topic of interest under the GDPR, US HIPPA, etc.
- Talent inside an organization (e.g., Privacy champions) can be an effective voice of business
- Encourage and incent Privacy champions and reps to get IAPP certifications
- A Privacy project manager can be a very strong asset to an organization
- A combination of business, IT, and legal knowledge makes strong privacy leaders
- Privacy leaders are responsible for tapping and nurturing talent within their organizations
- As no one really knows what “compliance” means, aim for “defensible position”
- Maturity models across businesses vary with risks and use of third-party vendors

6. DPO -- In-house or external

- Use an external DPO (data protection officer) who has a good working relationship with data protection authorities (DPAs), works councils, and who has the requisite Privacy and security expertise
- In-house Privacy teams typically handle Privacy-related reporting requirements
- A 50/50 mix of internal vs. external DPOs is seen in organizations these days
- An external DPO is typically used for escalations and law interpretation, not operational matters
- External DPO roles should be carefully defined, with outsourcing costs clearly understood
- Internal DPO appointments are preferred to promote organizational accountability, with outside counsel used for legal support
- An internal DPO should have deep subject matter expertise, as well as experience operationalizing Privacy
- An organization's DPO and Privacy resource requirements depend on its size and complexity
- No one size fits all

Questions from Audience

Q1. Specific examples on how GDPR readiness has impacted privacy programs?

Workstreams, third-party risk management, GDPR Article 28 processor requirements, vendor vetting, working with Information Security and vendors, and understanding geographic scope.

Q2. Which domain of GDPR readiness, privacy program rollout took up most resources?

Breach management, data subject rights, data subject access requirements (DSAR), using AI (artificial intelligence) to scan contracts that require Privacy language, involving CFO/Finance for funding support, ensuring executive-level visibility, understanding the big impact of IT and Information Security, Privacy as not just a legal project, and ensuring accountability at all levels.

PANEL 2: Operationalizing Global Privacy & GDPR Requirements

1. **Privacy by Design** (PbD) and **Security by Design** (SbD)

- Privacy by Design (PbD) is a new concept to many in European countries, even though it has been around for a while
- PbD certifications are not currently available; regulators are still working on certifying certifiers
- Baking PbD into products from the beginning saves money in the end
- Privacy is a differentiator if an organization's product design is a Privacy-enabler for customers
- PbD involves audit of product/tools/processes, reviewing notices, data collection sites, geo-filtering (esp. Canada and Germany) and tweaking Privacy notices
- Security is viewed as an area that is more focused on physical, technical, and administrative controls
- Privacy weaves in transparency, as well as social and human interaction components
- The ethical component of Privacy is understanding products in the context of human rights
- SbD is a legal requirement in US, with media attention focused on data breaches and associated fines
- The more mature SbD can be a push for PbD -- PbD is on a trajectory to attain SbD status/recognition

2. Data Privacy Impact Assessment (DPIA)

- A Data Protection Impact Assessment (DPIA) can be considered more of a philosophy
- It focuses on customers, a global approach, Privacy notices, security, privacy, and data sharing
- Some German regulators have released lists of what should be in a DPIA
- There is uncertainty on whether DPIAs have to be translated into local languages; if local regulators ask for a translation, it has to be provided
- Need to include translation budget for DPIA requests (e.g., Germany tends to ask for translations)
- Allocate resources for managing the DPIA process and for translations
- DPIAs may also include side projects that require outside consultant/contractor assistance
- Legal process outsourcing and administrative/legal consulting are very helpful for project management
- Vendor assessments may result in the removal of some non-compliant vendors, with budget implications
- IT budgets should include the migration cost of switching vendors from post-DPIA findings

3. Consent Management

- Involve Product teams in assessing consent management tools to purchase
- Marketing teams can use audit materials to create e-books/guides on the handling of consent and to meet accountability requirements
- Customers always welcome tools and process guidance provided by organizations
- Consult with legal counsel on questions related to legal bases for processing activities
- Review all applicable notices and data collection sites; archive information per recordkeeping rules
- Geo-filtering for different countries' consent requirements is an area that can turn into a big project

4. Records of Processing Activities (ROPA)

- Use a business process approach
- As data rarely flows in straight lines, an applications-only approach is not sufficient or realistic
- Maintain a list of tools/applications/systems as a safety net
- Use third-party tools with easily-customizable questionnaires
- Include interviews as part of the process; ask lots of follow-up questions to get the full picture
- Conduct data mapping properly to get the right information; also consider regulatory changes
- Map data flows within the entire organization
- Involve IT to conduct full-scale review of entire cloud architecture, vendors used, collection points, etc.
- Marketing and Sales can help locate sites collecting or storing information no longer needed
- An Architecture Review Board can meet quarterly to review tools and ensure everything is up to date
- Be ready to demonstrate to regulators the organization's reasonable records of processing practices

5. Individual Rights

- Start with people, process, and then tools
- Build a low-tech process that is followed by change management, before automating
- Many third-party tools are available
- Ensure clear process flows for requests; notification processes should also be quick and thorough
- Need to understand and document processes that cover data subject types, personal data types, processing location, data transfers, etc.
- A CMDB (configuration management database) tool can be used to validate records of processing
- For "Right to be Forgotten" requests, get clear and accurate answers from data subject; if doubtful about the request falling within organizational guidelines, consult with legal counsel
- Germany has certain guidance on proving someone opted in, removing them, etc.
- Don't respond to requests without going through proper verifications to validate requestor's identity

Questions from Audience

Q1. Are you seeing common threads about global operations beyond GDPR?

- GDPR considered by many to be the gold standard that will meet many country/local requirements
- Reviewing and comparing region/country/local laws to make sure nothing is missed
- Keeping track of local regulatory changes, trends, and data localization laws
- Creating global heat maps about customer locations and the organization's online presence
- Data retention is a hot potato - from policy implementation, daily business operations, to audits
- Purchasing tools for email and setting up proper email retention policy
- Retention requirements for employee data being significantly different for each EEA country
- For HR tools, adopting principle of protecting employee data and deleting what is not needed

Q2. Are there other items in budget?

- Translations
- Fees for legal consulting and GDPR readiness project management
- Vendor assessments that result in removing vendors, due to their weak data protection posture
- IT budget for offboarding vendors that do not make the cut, and onboarding replacement vendors
- Licensing of new Privacy tools to automate processes
