IAPP : The New Technologies Approach to Privacy
Top Ten Privacy Issues in Cybersecurity to Watch for in 2017

Ari Schwartz
Managing Director of Cybersecurity Services
Venable LLP
aschwartz@venable.com/202-344-4711
10) Privacy Engineering

- Privacy By Design has become increasingly important concern for cybersecurity tools
- Privacy Engineering ties into basic risk management
- NIST released a new report in January for Federal Systems, but with broader application
9) Data Breach Reporting

- Bi-partisan support for passing a federal notice statute pre-empting states
- Biggest hold up has always been Congressional jurisdiction

- Sectors that have disagreed in the past seem closer to consensus language
- Has been a perennial top ten issue for over 13 years
8) Identity Management

- Recent Breaches have highlighted the importance of multifactor authentication and move away from the password
- Privacy issues and ease of use are key to greater adoption
Last year, the European Union passed a directive on security of networked and information systems.

Critical infrastructure (CI) must report breaches promptly.

CI definition is broader than in the US.

Coupled with General Data Protection Rule (GDPR), companies with business in Europe have greatly increased privacy and security compliance obligations.
6) CISA Compliance

- Cybersecurity Information Sharing Act was signed into law in December 2015.
- Allows for sharing of cyber threat info notwithstanding any other provision of law.
- New privacy rules apply in guidance from DHS and DOJ.
CISA made Threat Sharing easier

Many security officers now would like to see more analysis shared

Raw data and analysis have different privacy concerns

Much less has been written about how do share cyber analytics that involves PII
4) Rules on Hack Back

- During the CISA debate, many companies pushed for clarity on hack back rules
- Drafts providing language attempting to explain current rules were not accepted
  - Organizations can take many steps to stop attackers on their own systems
  - Very little that organizations can do on other systems
- Companies continue to push into gray areas in order to stop future hacks
3) Encryption Policy

- President Trump expressed concern over US encryption policy during the campaign.
- FBI Director Comey has asked for “An Adult Conversation” on encryption.
- Joint House Committee Report found that Backdoors harm cyber security and raise privacy concerns.
2) Vulnerability Disclosure

- Organizations continue to move toward creating disclosure policies to create certainty in how they receive information about vulnerabilities.

- Some have developed bug bounty programs, including:
  - All major Internet Companies
  - Many leading software and hardware providers
  - US Army

- Rules on what researchers can do include privacy direction.
1) Government Hacking

- In 2016, San Bernadino iPhone Case awoke many policymakers to this issue.

- US government has Vulnerabilities Equities Process that has been both praised and criticized.

- Should governments be encouraged to hack?

- Many other governments are coming up with their own rules: Netherlands, Italy, etc.
Questions?

Ari Schwartz  
Managing Director of Cybersecurity Services  
Venable LLP  
aschwartz@venable.com
Engineering Privacy: A Primer

Peter F Brown, CIPT
Owner, Principal
Peter F Brown Consulting bvba
@PensivePeter
Goal

- Understanding how to deliver privacy-compliant, accountable systems and applications in the global data sphere
  - Can privacy protection become more science and less art?
  - Can this become a distinct discipline?
  - Is it something InfoSec professionals should care about?

*Which beg the questions:*
  - What is ‘privacy’?; and
  - Can it be ‘engineered’?
Privacy: Easy, peasy – right?

- collection limitation
- data quality
- purpose specification
- use limitation
- security safeguards
- openness
- individual participation
- accountability

... yada yada

*From “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”*
Wrong!

- Different jurisdictions, regulations, rules
- Differing expectations – personal, societal, commercial
- Different incentives – rewards and punishments
- Differing definitions, terminology
- Different disciplines involved – risk, compliance, InfoSec, governance
- Increased complexity – volume, speed, trajectory, flows

Is it actually all too nebulous?
Starting from:

*If...*

- ‘Personal data does not exist’
- ‘privacy engineering does not exist’

*what exactly are we doing here?*

- Useful to make some distinctions between:
  - analogue and digital;
  - data and information;
  - data protection and privacy
Analogue vs Digital

- Information *always* has context or supporting medium
  - an “analogue” connection with the real-world
  - the information has a *visceral connection* with reality

- Data does not: for it to become information, something happens
  - Digital ‘intermediation’ by processes, systems, interfaces
  - information is *derived* from a model – not necessarily from reality!
Data “just...is...”

- “23” is data
- “06dc5e2e229cf0c15a99f2e01ace9ec7” is data
- Data – on its own – has no impact on the world
  - “23” doesn’t mean anything
- Data in context – in formation – does
  - “it is currently 23° Celsius in this room” does
Data Protection vs Privacy

- Data protection is “only” ever a (digital) systems phenomenon
  - This *can* be engineered

- Privacy is always a real world (analogue) phenomenon
  - It cannot be engineered
What do we mean by “Privacy Engineering”? 

- Consensus on “engineering”
  - as a discipline

- But “privacy engineering”:
  - What is it?
  - Can we *really* do it?
Role of Standards – reducing risk

In particular...

- OASIS Privacy Management Reference Model & Methodology (PMRM)
- ISO 19944 (Data and their flow between cloud services and devices)

(many other sources and tools
- OASIS PbD-SE, ISO 29100, 31000, Guide 73, 38505; NIST 800-53, NISTIR 8062, OMB circular A-130...
The OASIS Privacy Management Reference Model and Methodology
PMRM Model

1. Privacy Controls
   - Influence
   - Conform with

2. Laws & Regulations
   - Inform

3. Policies
   - Drive
   - Responsible for
   - Applied by

4. Stakeholders
   - Express

5. PMRM Services
   - Manages
   - Used within

6. Technology
   - Supports

7. Privacy Domain
   - Manage

8. Privacy Architecture
   - Inform

9. Use Cases
   - Represented in
   - Develop

10. Core Concerns (protection of PI/PII)
ISO 19944

Data and their Flow between Cloud Services and Devices
(entering final approval stages in ISO/IEC JTC1 SC38)
ISO 19944 – Data Taxonomy

- A standardized taxonomy
- types of data, qualifiers, processes, uses and scope of use
ISO 19944 – Data Usage Statements

- **Standardized statement structure**
  - Engineer the creation, processing and parsing of standard usage statements
  - Build a bridge between software engineering and legal/conformance/corporate requirements
What you can do

- Inform yourself of:
  - Your privacy management environment and compliance objectives;
  - Who at C-suite level champions data protection and privacy as a corporate issue;
  - What standards are out there to help you

- Use the PMRM:
  - to identify weaknesses or shortcomings of current policies;
  - to identify privacy control requirements;
  - to establish best practice guidelines where needed

- Use ISO 19944:
  - to identify data flows;
  - to create data usage statements
Bibliography

- OASIS Privacy Management Reference Model and Methodology
  http://docs.oasis-open.org/pmrmd/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html

- ISO 19944, 29100, 31000, 38505, Guide 73
  http://www.iso.org/iso/home/standards.htm

- NIST Risk Management Framework

- NISTIR 8062 Introduction to Privacy Engineering and Risk Management in Federal Systems
  https://doi.org/10.6028/NIST.IR.8062

- OECD
  http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
Time for a Break!
Emerging Privacy Technologies for the Enterprise

MODERATOR: Jedidiah Bracy, CIPP
Editor
IAPP

PANELISTS:
Kabir Barday, CIPP/US, CIPM
CEO
OneTrust

Peter Cranstone
CEO
3PHealth

Nimrod Luria
CEO
Prifender
VP and CPO
TRUSTe

Hilary Wandall
2016 IAPP Privacy Tech Vendor Report
What is it?

- 3,500+ word report, which discusses trends in the use of technology by privacy pros to help with their operations, defines categories of vendors, and offers some thoughts on the direction of the market

- Listings of 45 vendors, laid out with logos, screenshots, links to their sites, 100-word descriptions, names of leadership, HQ location, etc.

- Plus, each company it categorized in one of two ways:
Categorization of Vendors

- **PPM vs. EPM:**
  - PPM – Privacy Program Management: Tools used by the privacy team, which can be used without huge IT lift or org-wide involvement
  - EPM – Enterprise Privacy Management: Tools needing significant IT installation, network-wide impact, uses often beyond privacy

- **PPMs:** Assessment managers, consent managers, website scanning, breach response
- **EPMs:** Data discovery, data mapping, activity monitoring

- **ALSO:** De-identification and enterprise communications
One Trust

Location: Atlanta, GA; London, U.K.
Number of Employees: 51-200
Founded: 2016
Leadership: Kabir Barday, CEO; John Marshall, Alan Dabbiere, Co Chairman; JP Halebeed, Global R&D; Andrew Clearwater, Director, Privacy; Chris Hoff, Director, Regulatory Affairs
Funded: Self-funded
Privacy-related products: Data Discovery, Data Mapping, Assessment Manager, Website Scanning, Consent Management

Description: OneTrust offers a privacy management software platform designed to help organizations comply with data privacy regulations across different sectors and jurisdictions, including the GDPR and Privacy Shield. It provides assessment automation tools for PIAs, DPIAs, and vendor-risk assessments; maps data to provide a central register of data flows, processing, and reporting; scans sites for cookie compliance; and certifies for Privacy Shield and APEC CBPR commitments. The platform offers dashboards, metrics, and reports for companies to track their progress.
Why we’re doing it

- This is genuinely helpful to the members. They’re shopping for this stuff and this helps them compare apples to apples and ask smart questions.

- Defining an industry and nomenclature helps it to come together and innovate faster. Also good for members – better solutions.

- These are “privacy” solutions, which are bought and used by privacy pros, not “IT” or “security” solutions, bought and used by those teams.
OneTrust
Privacy Management Software
OneTrust.com/request-demo

Kabir Barday
OneTrust, CEO
kbarday@onetrust.com
Privacy as a Competitive Advantage
Choice and Trust are the Keys to Value Network Monetization
We Have a History of Solving Big Problems with *Simple* Innovation
Two De Facto Standards and One Web Standard

**Internet Performance**
2000

We Made the Internet Faster
500+ Million Installations (Mod_Gzip)

**Internet Security**
2006

We Made the Internet More Secure
Protecting 85% of the Internet’s Reverse DNS (rDNS) requests – Source T

**Internet Privacy**
2012

We Made the Internet Private
1.5+ Billion Installations (DNT browser function)
Our Latest *Simple* Innovation

We’ve made the Internet *more* Personal

**Net Effect**

We now have the *foundational tools* to enable contextual computing, starting with Privacy

*Contextual Data Communications Platform U.S. Patents: 7,873,710 – 8,156,206 – 8,725,851 – 8,959,190*
Today’s Privacy Imperative

New privacy regulations require the Web to Recognize, Respect and Respond to each user’s personal context to ensure meaningful consent
Aligning the Stakeholders

The Consumer and the Enterprise Need Better Privacy/Security Choices

Choices that...

- Leverage technology to support lower cost business models and connect economically coherent value networks
- Utilize a privacy-by-design framework, that adapts to any country/region/industry and aligns all stakeholders
- Allow ME to expressly consent to the collection, flow, use, and assignment of MY personal data in the moment
- Are Contextual
Choice®
A Web-Standards Framework for Privacy Centric Communications

Provides a simple navigation solution and single point of access to cost effectively enable an individual’s privacy needs based on their personal choices and environment.

Web Standards Approach
Responsive User Interface. Presents and connects the user with the most appropriate digital channel for their current needs

Individualized Navigation
Responsive User Interface. Presents and connects the user with the most appropriate digital channel for their current needs

Respects Me
Deliver the appropriate content and services based upon each individual’s unique data sharing preferences

Seamlessly Connect
One app connects people, content, services and devices across evolving, distributed IoT networks

Meaningful Impact
The data you need to determine usage, compliance, operational and financial impact
Choice®
Automating Consent Based Privacy

Proftable Business
Strategy = Add a New Service

Request
Management identifies needed, profitable services and capabilities for any segment of their user and/or consumer base

Execute
IT updates AI/rules engine and accesses services or third party APIs. Solution delivered as a mobile optimized Web service

Monetize
Enables an economically coherent network that builds value within a privacy-centric, plug and play delivery model

Your Current IT Architecture

Digital Services Delivery Web Site

Required Protocols/Standards: HTTP/HTTPS/HTML/CSS/JavaScript/CGI
Incoming encrypted consent arrives via HTTP Request
Outgoing contextual response via HTML

Existing AI/Rules Engine

Channel’s Existing & New IoT Devices/Services

Existing & New Digital Services

API’s

Existing Digital Infrastructure

Existing Digital Backend Systems

+ Privacy and Respect

Access a New Service

Android and iOS
A private, secure, individualized GDPR compliant digital experience - all via a Responsive User Interface

Delivering On Your Business Strategy
A low cost innovative business model built on ‘negotiated digital commerce’

© 2017 3PHealth
DEMONSTRABLE **COMPLIANCE** THROUGH **IDENTITY-AWARE** TECHNOLOGY
ABOUT PRIFENDER

Prifender is using artificial intelligence technology to discover and map personal information across networks and systems, both structured and unstructured, while associating identities with their respective obligations so organizations can better manage and demonstrate accountability and compliance.
The Uniqueness of Our Product

- Privacy Context - Associating Identities with Obligations
- Automated PII Discovery and Data Mapping
- Using Artificial Intelligence Algorithms
- Built for Scale
- Powerful Analytics and Reporting Capabilities
“SHOW ME EVERYTHING YOU HAVE ON JOHN SMITH”

INVENTORY
An accurate listing of the personal information.

CROSS BORDER TRANSFERS
Identify what data is moving between geographies.

DISCLOSURES
Track which identities are shared with a third party.

REGULATIONS
Associate identities with the regulations that apply to them.

AUDITING AND MONITORING
Audit the activities associated with the identities of interest.

NOTICE MANAGEMENT
Associate each identity with the relevant notice.

DATA FLOWS
Track how identities move between systems, employees and suppliers.

CHOICE AND CONSENT
Associate choices made by data subjects across repositories, products and services.

ACCESS AND DELETE
Address requests to review records, update identifiers and manage deletion workflows.

RETENTION AND DISPOSAL
Identify files containing personal information that can be archived or deleted.

DATA QUALITY
Maintain accuracy across repositories by updating the identifiers.

POST BREACH IMPACT ANALYSIS
Identify the identities impacted by a breach.
Scaling Enterprise Privacy through Technology

From Policy to Accountability

Hilary Wandall, General Counsel & CDGO

13 February 2017
Technology Continues to Transform our Lives...

...and create new privacy and data governance challenges for organizations
Since the mid 1990s
Primary Focus on Traditional Legal, Policy & Regulatory

Legal Advice & Regulatory Guidance
Privacy Files
Scanning Tools
Spreadsheets
Surveys
Email
Action Plans

Internal
Government Affairs and Legal Teams

External
Law Firms
Consulting Firms
Policy Orgs
TRUSTe – Est. 1997
~20 year history of privacy solutions innovation

1998 – 2008
Privacy Certification and Verification Solutions
- Websites
- U.S.-EU Safe Harbor

2008 – 2011
Online Tech Solutions
- Mobile Apps Certification
- Cloud Certification
- Website & App Scanning Tools

2011 – 2013
Compliance Tech Solutions
- Ads Compliance
- Consent Management
- Website Monitoring

Comprehensive Platform
- Data Governance, Inventory & Mapping
- Regulatory and Enterprise Assessment Automation and Program Management
- Data Transfer Solutions (Privacy Shield, BCRs, APEC)

Regulatory Interoperability
Thank You

hilary@truste.com
Emerging Privacy Technologies for the Enterprise

MODERATOR: Jedidiah Bracy, CIPP
Editor
IAPP

PANELISTS:
Kabir Barday, CIPP/US, CIPM
CEO
OneTrust

Peter Cranstone
CEO
3PHealth

Nimrod Luria
CEO
VP and CPO
Prifender

Hilary Wandall
CEO
VP and CPO
TRUSTe