SQUIRE PATTON BOGGS

Practical Privacy By Design

March 21, 2023, 11:00 - 11:40 am ET

Speakers

Brittany Powell
Senior Manager Privacy & Compliance
The Coca-Cola Company

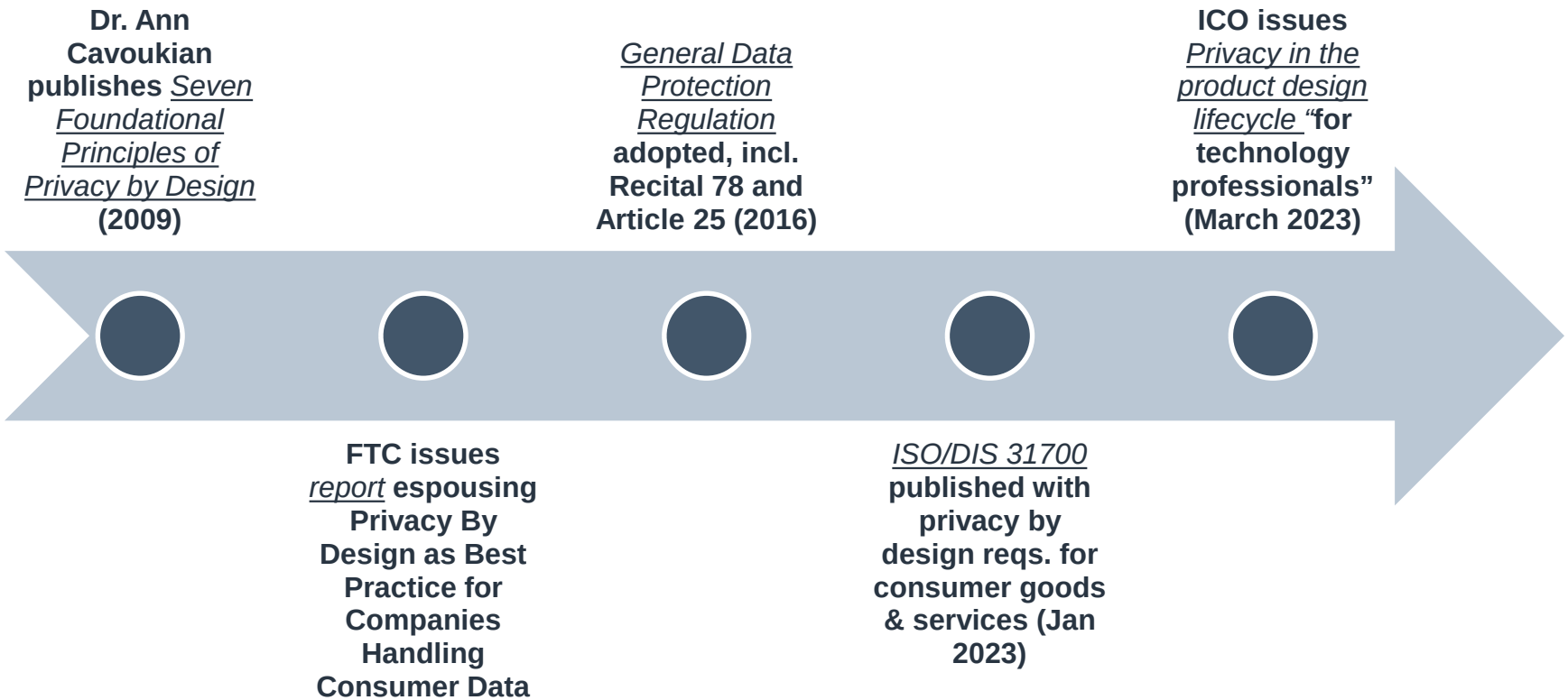
Dr. Annette Demmel
Partner, Squire Patton Boggs
Berlin

Julia Jacobson
Partner, Squire Patton Boggs
New York

SQUIRE PATTON BOGGS

Defining Privacy by Design

Brief Chronology of “Privacy By Design”



Cavoukian's Seven Foundational Principles of Privacy by Design*

SQUIRE PATTON BOGGS

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality — Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

*Source: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (Jan 2011)

SQUIRE PATTON BOGGS

Legal Requirements for Privacy by Design

Privacy By Design

SQUIRE PATTON BOGGS

- No universally recognized definition
- Not expressly defined in the privacy laws
- Proactive integration of privacy into the design and architecture of systems and business practices
- Privacy by Design is a cross-sectional process, not a state

Laws that Require Privacy By Design

SQUIRE PATTON BOGGS

GDPR Article 25: Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures … designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Key Privacy By Design Requirements

SQUIRE PATTON BOGGS

Role of Data Protection Impact Assessments

Focus on Data Minimization

- As Default Setting
- Embedded into Design
- Proactive not Reactive
- Preventative not Remedial
- Full Lifecycle Protection
- Visible

Data Minimisation in Practice

SQUIRE PATTON BOGGS

Excerpt of a DPIA on a fleet management and supply planning software

Categories of data	Why required?	Original desire for retention	Consequences?	Agreed retention
Employee master data	to set up the employee in the system	10 years after termination	full duplication of HR data	3 months after employee leaves
~~Employee private address~~	not required	10 years after termination		
Driving license class	organize transport	10 years after termination	full duplication of HR data	3 months after employee leaves
ADR license (carriage of dangerous goods)	organize transport	10 years after termination	full duplication of HR data	3 months after employee leaves
Delivery Note	proof of evidence	24 months		24 months
assigned order and tour data	organize transport	24 months		24 months
GPS position	organize transport, optimize current tour	24 months	full movement profile	end of a working day (23.59 hrs.)
Speed of the operating device	optimize future tour planning	24 months	full behavior control	end of a working day (23.59 hrs.)
geo-fencing	prevent difficulties	24 months	full behavior control	end of a working day (23.59 hrs.)
unloading time	optimize future tour planning	24 months	full behavior control	Anonymized at the end of a working day (23.59 hrs.)
total working time	working time registration	24 months		24 months
Photographs (transport related)	proof of evidence	2 months		2 months
Notes on damages, etc.	proof of evidence	2 months		2 months
Tachograph data	adherence to driving time restriction	24 months		24 months

U.S. Privacy Laws

Five U.S. State General Privacy Laws – not explicit but include elements

- California – CCPA Regulations §7002; considering the GDPR model for risk assessments
- Role of Privacy Impact Assessments (*n.b.*, almost final Iowa state privacy law does ***not*** require privacy impact assessments)
- Consumer Transparency and User Centricity

Proposed U.S. Federal Law - *American Data Privacy and Protection Act* **-** §103

- *consider applicable Federal laws, rules, or regulations related to covered data*
- *identify, assess, and mitigate privacy risks related to covered minors*
- *mitigate privacy risks …related to the products and services of the covered entity or the service provider*
- *implement reasonable training and safeguards within the covered entity and service provider to promote compliance with all privacy laws applicable to covered data*

Quebec – September 2023 - “ensure that the parameters of the product or service provide the highest level of confidentiality by default, without the intervention of the person concerned”

SQUIRE PATTON BOGGS

Practicing Privacy by Design

Practicing Privacy by Design

SQUIRE PATTON BOGGS

Principles in Action: getting the right controls in the right place at the right time

Establish:

- Privacy Resilient Controls
  - Transparency, e.g., where, what and when of privacy notices
- ‘Ownership’ for Privacy Resilient Controls
  - User centric - global *vs.* local decision-making
- Standards, processes and procedures to help ensure that Privacy Resilient Controls are:
  - Proactive
  - Repeatable

SQUIRE PATTON BOGGS

Starting Privacy By Design

Getting Momentum

SQUIRE PATTON BOGGS

- Ongoing: Privacy By Design begins but never ends

- Every organization has its own context for Privacy by Design
  - No one size fits all
  - No right or wrong way

Getting Momentum

SQUIRE PATTON BOGGS

- Leadership Commitment to Privacy by Design
  - Requires *genuine* commitment and *dedicated* resources
- Bottom-up and Cross-functional Engagement
  - Engage stakeholders
  - Leverage what's already in place, e.g., Security by Design

Getting Momentum: ISO 31700

SQUIRE PATTON BOGGS

- **ISO 31700-1 Consumer protection — Privacy by Design for Consumer Goods and Services — <u>Part 1: High-level requirements</u>**
  - *"[…] establishes **high-level requirements** for privacy by design to protect privacy throughout the lifecycle of a consumer product, including data processed by the consumer."*
  - *"[…] **does not** contain specific requirements for the privacy assurances and commitments that organizations can offer consumers nor does it **specify particular methodologies that an organization can adopt to design and-implement privacy controls, nor the technology that can be used to operate such controls**."*
  - "*The primary audiences for this document are those staff of organizations, and third parties, who are responsible for the concept, design, manufacturing, testing, operation, service, maintenance and disposal of consumer products or services*."
- **ISO 31700-2 Consumer protection — Privacy by Design for Consumer Goods and Services — <u>Part 2: Use cases</u>**
  - Provides three sample use cases: ecommerce, a fitness company and smart locks

SQUIRE PATTON BOGGS

Questions?


Thank You!

Global Coverage

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Dubai
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Milan
New Jersey
New York
Palo Alto
Paris
Perth
Phoenix
Prague
Riyadh
San Francisco
Santo Domingo
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico

Office locations
Regional desks and strategic alliances