

Jason Cronk's *Strategic Privacy by Design* sets forth a clear, comprehensive, and highly practical blueprint for incorporating privacy into design. Cronk deftly explains the dimensions of privacy in a sophisticated way that is enlightening not just to novices but also to seasoned experts. Cronk's copious use of concrete examples is some of the very best I've seen. Well-organized and accessible, this book has numerous helpful charts and illustrations. This book is an essential resource for engineers as well as privacy professionals.

– Prof. Daniel Solove, *George Washington University Law School and President of TeachPrivacy*

Having created Privacy by Design so many years ago, it is truly heartwarming to see a book dedicated to exploring its application and breadth! Jason has done an excellent job in outlining the value of proactively embedding privacy into the design of one's operations, in an effort to prevent the privacy harms from arising. Jason's book will no doubt become a welcome addition in many jurisdictions

– Ann Cavoukian, *Ph.D., Three-term Information and Privacy Commissioner of Ontario, Canada, Distinguished Expert-in-Residence, Privacy by Design Centre of Excellence, Ryerson University*

This book is a formative piece of work. Individually I've read Cavoukian, Solove and Nissenbaum, but Jason introduces Hoepman among others and then blends their concepts, resulting in a framework that is pragmatic, thorough and probably quite different from most of the other approaches you may have come across.

– Tim Clements, *Program Manager, Copenhagen*

Jason operationalizes the seven PbD principles into a practical formula that links privacy threats and controls into a repeatable framework. The approach holistically integrates legal and philosophical foundations of privacy with practical technical controls and mitigations that engineers can apply, today.

– Prof. Travis Breaux, *Editor of Introduction to IT Privacy*

Cronk's book provides a strong foundation for analyzing potential privacy issues in the design of products and services, and I have already started using some the strategies and the thought-provoking examples when I create internal frameworks and hold training sessions. I highly recommend it for anyone looking for a constructive, structured and repeatable approach to PbD.

– Lars Vinden, *Corporate Privacy Counsel/DPO, Telia Norge*

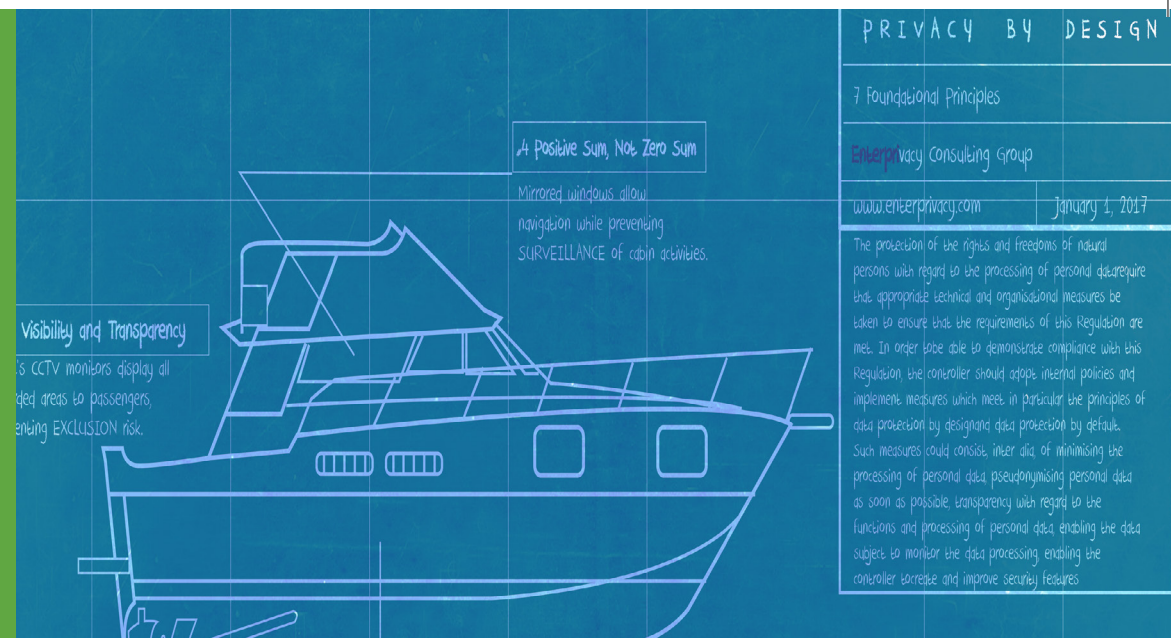


R. Jason Cronk began his interest in privacy in the early 1990s when his roommate, a private investigator, introduced him to the world of data brokers. Years later, working in information security, he went to law school to turn his passion for privacy into a career. Jason became an active member of the privacy community through the IAPP, writing and speaking on the need for privacy engineering and design. Early on, the IPC of Ontario, Canada designated him a PbD Ambassador for his advocacy. When not helping clients at his boutique consulting practice, Enterprivacy Consulting Group, he can be found tweeting @privacymaverick



An **iapp** publication

STRATEGIC PRIVACY BY DESIGN



STRATEGIC Privacy By Design

R. Jason Cronk
CIPP/US, CIPM, CIPT, FIP

iapp

An **iapp** publication

Contents

SECTION I: INTRODUCTION

Foreword xi

Many Thanks xv

Chapter 1: What Is Privacy by Design?

The 7 Foundational Principles 2

Principle 1: *Proactive*, Not Reactive; *Preventative*, Not Remedial 2

Principle 2: Privacy as the *Default* Setting 3

Principle 3: Privacy *Embedded* into Design 4

Principle 4: Full Functionality — *Positive Sum*, Not Zero Sum 5

Principle 5: End-to-End Security — *Full Life Cycle Protection* 6

Principle 6: *Visibility* and *Transparency* — Keep It Open 7

Principle 7: *Respect* for User Privacy; Keep It *User Centric* 8

Short History of Adoption 8

2009 8

2010 9

2011 9

2012 9

2015 10

2016 10

2018 11

Challenges of the Principles 12

Why It's Important to Build in Privacy 13

Structural Asymmetry 13

Cognitive Biases 14

SECTION II: PRIVACY MODEL

Chapter 2: Actors

Individuals.....23

Domain/Threat Actors26

Relationships30

 Example 1: An interactive online multi-player game.....32

 Example 2: Human resources department vetting job candidates
 through an online skill-testing service33

 Example 3: Political activist website.....34

Chapter 3: Violations

Information Collection42

 Surveillance42

 Interrogation.....43

Information Processing45

 Aggregation.....45

 Insecurity46

 Identification48

 Secondary Use49

 Exclusion52

Information Dissemination54

 Breach of Confidentiality.....54

 Disclosure55

 Exposure56

 Increased Accessibility.....57

 Blackmail.....59

 Appropriation.....60

 Distortion.....62

Invasions63

 Intrusion.....63

 Decisional Interference64

Decisional Interference through Dark Patterns.....67

Chapter 4: Controls

Architecture	79
Identifiability	81
Centralization	86
Strategies	88
Architecture Redux	117

Chapter 5: Information Flow, Domains and Subdomains

Information Flow	127
Domains and Subdomains	135
Example and Exercises	140
Pothole App	140
Exercises	145

SECTION III: ANALYSIS

Chapter 6: Consequences

Privacy Harms	153
Subjective Harms Examples	156
Objective Harms Examples	157

Chapter 7: Risk Analysis

A “FAIR” Method for Privacy Risk	166
Frequency	171
Attempt Frequency	172
Vulnerability	175
Magnitude	177
Applying Controls	189
Organizational Risk	194
Domain Redux	195

Chapter 8: Quantifying Risks

Risk of Exposure in a Restaurant Bathroom	201
Opportunity Frequency	203
Probability of Action	203

Attempt Frequency	203
Vulnerability	204
Action Frequency	205
Population Magnitude	205
Risk	206
Adverse Consequence Risk	207
Risk of Secondary Use of U.S. Census Data	208
Opportunity Frequency	209
Probability of Action	209
Action Frequency	210
Vulnerability	211
Action Frequency	211
Population Magnitude	212
Risk	212
Example and Exercises.....	215
Pothole App.....	215
Exercises	222

SECTION IV: METHODOLOGY

Chapter 9: Methodology

Baking in Privacy	230
Identify the Purpose	230
Understand Quality Attributes	232
Identify Information Needs	233
Imposing Controls	235
Architect.....	236
Secure.....	239
Supervise	240
Balance	241
Online Behavioral Advertising	243

Integrating Privacy by Design into the Business	245
Accountability	245
Awareness	246
Expertise	246
Chapter 10: Final Thoughts	
Privacy-by-Design Redux	251
Principle 1: <i>Proactive</i> , Not Reactive; <i>Preventative</i> , Not Remedial	251
Principle 2: Privacy as the <i>Default</i> Setting	252
Principle 3: Privacy <i>Embedded</i> into Design	252
Principle 4: Full Functionality — <i>Positive Sum</i> , Not Zero Sum	253
Principle 5: End-to-End Security — <i>Full Life Cycle Protection</i>	254
Principle 6: <i>Visibility</i> and <i>Transparency</i> — Keep It <i>Open</i>	254
Principle 7: <i>Respect</i> for User Privacy; Keep It <i>User Centric</i>	255
Example and Exercises	257
Pothole App	257
Exercises	259