

Privacy by Design

Introduction to Privacy Engineering
Daniel Aranki
University of California, Berkeley

Privacy by Design

Introduction: Genesis

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Readings

Relevant reading: [Ann Cavoukian \(2012\)](#). "Privacy by design: origins, meaning, and prospects for assuring privacy and trust in the information era". In: [Privacy protection measures and technologies in business organizations: aspects and standards](#). IGI Global, pp. 170–208.

Myths/Misconceptions About Privacy

- “Privacy is dead.”
- “I have nothing to hide.”
- “No one cares about privacy.”
- “More security/safety means less privacy.”
- “More utility means less privacy.”

Data

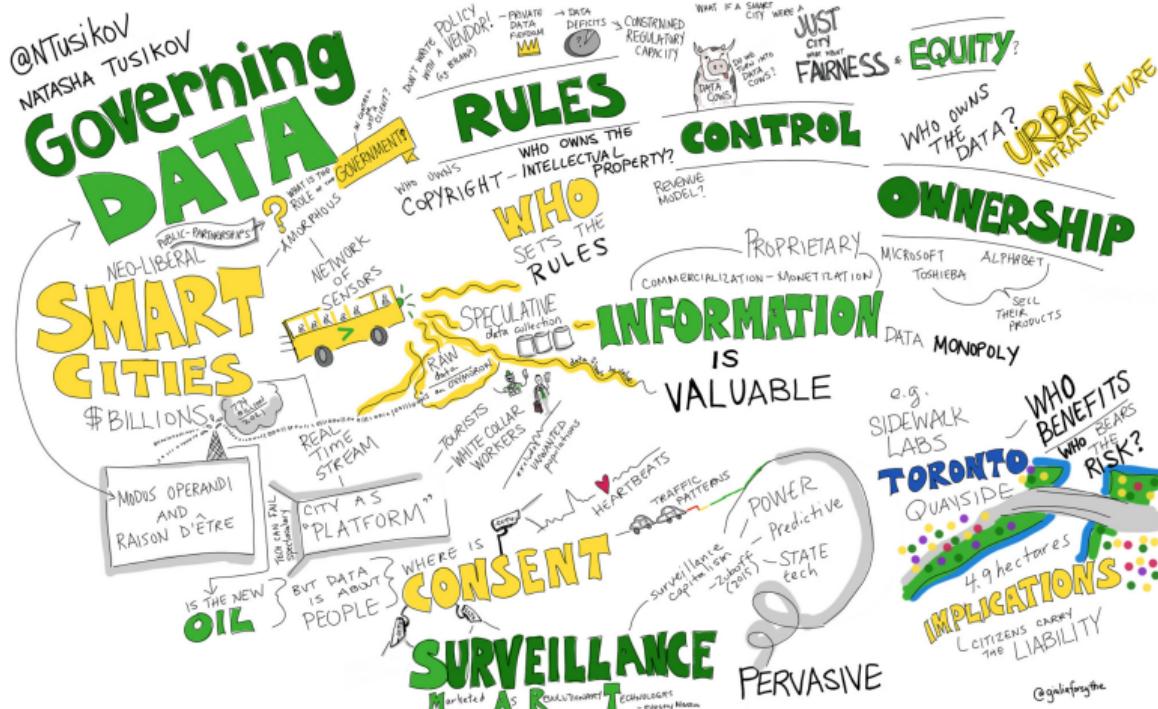


Figure: “Data Governance” by Giulia Forsythe, CC BY 2.0

What is Privacy by Design?

- Concept developed by Ann Cavoukian (former Information and Privacy Commissioner of Ontario)
- Building privacy principles into everyday operations
- Shift of burden of privacy protection away from consumer and towards business/entity
- Privacy by design accepted as an international standard (e.g., GDPR)



Figure: "Please Keep Door Locked" by Steven Depolo, CC BY 2.0

The Principles

- Proactive not Reactive
- Privacy as the Default Setting
- Privacy Embedded into Design
- Positive-Sum Philosophy
- End-to-End Security
- Visibility and Transparency
- User-Centric Design



Figure: “System Lock” by Yuri Samoilov, CC BY 3.0

Privacy by Design

Proactive Not Reactive: Principle

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Principle

- Think about privacy from the beginning
- Don't wait until there's a breach
- Be proactive about privacy: anticipate
- No guidelines to resolving infractions after-the-fact (remedy)
- Privacy is an ongoing endeavor
- Always think about privacy

Example: E-Mail

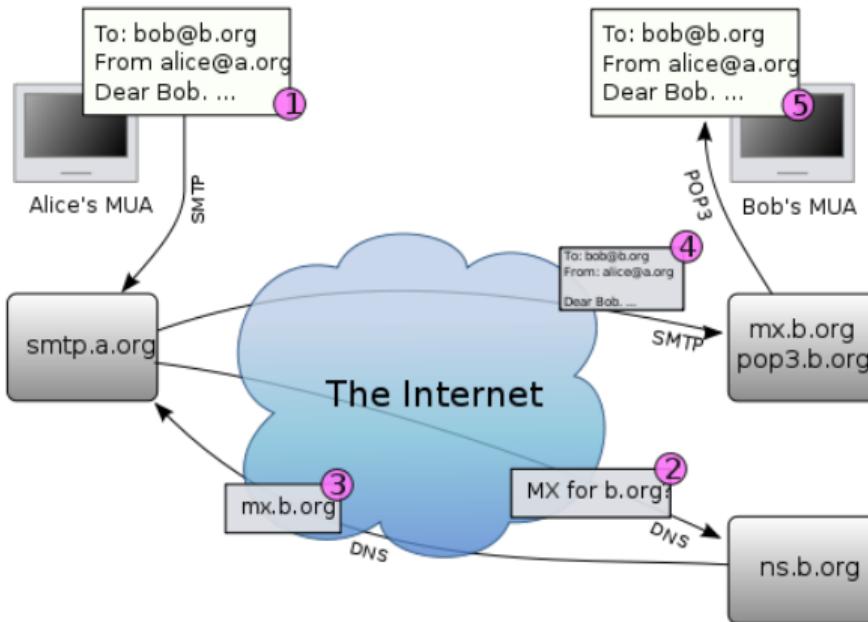


Figure: “Email Operation” by Yzmo, CC BY-SA 3.0

Privacy by Design

Privacy as the Default Setting: Principle

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Principle

- Out of the box: privacy-aware
- Even without taking any action, individuals are protected
- Opt-in vs opt-out
- Users may still change these settings
- Relationship to consent



Figure: Privacy by default

Example: Flashlight App



Figure: “Flashlight Clear” by Mrmariokartguy, CC BY-SA 4.0

Example: Social Networks

The screenshot shows the Facebook Privacy Settings and Tools page. The left sidebar lists various sections: General, Security and Login, Your Facebook Information, Privacy (selected), Timeline and Tagging, Location, Blocking, Language, Notifications, Mobile, Public Posts, Apps and Websites, Instant Games, Business Integrations, Ads, Payments, Support Inbox, and Videos. The main content area is titled "Privacy Settings and Tools". It is divided into two sections: "Your Activity" and "How People Find and Contact You".

| Category | Setting | Value | Action |
|---------------------------------|---|----------|------------------|
| Your Activity | Who can see your future posts? | Friends | Edit |
| | Review all your posts and things you're tagged in | | Use Activity Log |
| | Limit the audience for posts you've shared with friends of friends or Public? | | Limit Past Posts |
| How People Find and Contact You | Who can send you friend requests? | Everyone | Edit |
| | Who can see your friends list? | Public | Edit |
| | Who can look you up using the email address you provided? | Everyone | Edit |
| | Who can look you up using the phone number you provided? | Everyone | Edit |
| | Do you want search engines outside of Facebook to link to your profile? | Yes | Edit |

Figure: Facebook default privacy settings

Privacy by Design

Privacy Embedded Into Design: Principle

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Principle

- Privacy embedded into design of system/product; **not** as an add-on to the system/product
- Privacy is an essential component at the moment of design and throughout life of the system/product
- Particularly important in context of government data, where individual does not “consent”

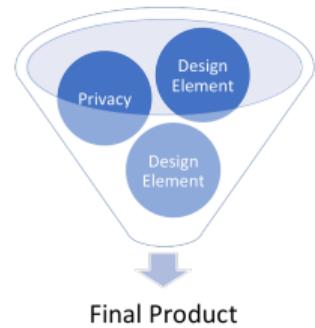


Figure: Ingredients system design

Example: GPS



Figure: Global Positioning System (GPS) satellite

Privacy by Design

Full Functionality – Positive Sum: Principle

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Principle

- False dichotomy: privacy vs. security
- Privacy-utility trade-off
- Positive-sum game **not** zero-sum!
- Accommodates all legitimate objectives
no unnecessary trade-offs



Figure: Privacy trade-offs

Example: Berkeley Telemonitoring



Figure: Berkeley Telemonitoring Project

Example: Private Disclosure of Information

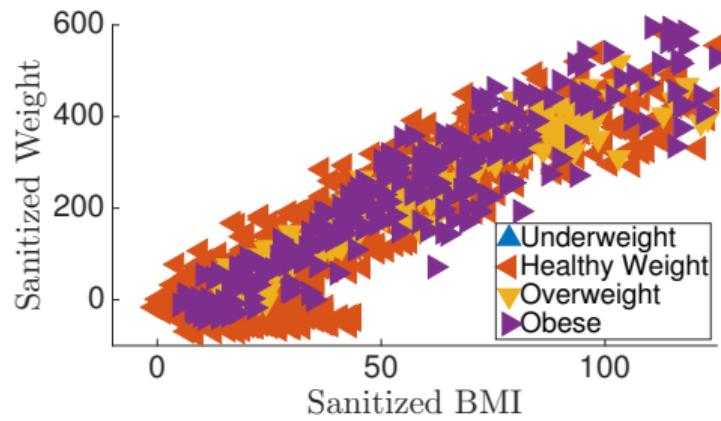
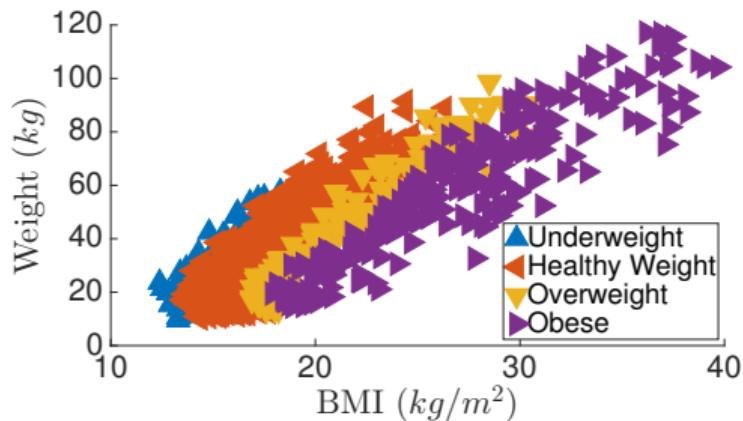


Figure: Sanitizing data using PDI

Privacy by Design

End-to-End Security – Full Lifecycle Protection: Principle

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Principle

- Extends throughout entire lifecycle of data; both:
 - Temporally; and
 - Spatially
- Cradle to grave: secure retention, transmission and processing; and secure destruction



Figure: “Safe On The Footpath” by William Murphy, CC BY-SA 2.0

Example: Electronic Health Record



Figure: “Health Showcase” by Juhan Sonin, CC BY 2.0

Privacy by Design

Visibility and Transparency: Principle

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Principle

- Follow through on promises and objectives
- Subject to independent (and internal) verification
- Visibility and transparency to users and providers
- Right to be forgotten
- Right to access and scrutinize one's data



Figure: "Jar With Stones" by Marco Verch, CC BY 2.0

Example: GDPR



Figure: “GDPR” by Dennis van der Heijden, CC BY 2.0

Privacy by Design

Respect for User Privacy – Keep it User-Centric: Principle

Introduction to Privacy Engineering

Daniel Aranki

University of California, Berkeley

Principle

- Inclusion of measures that protect interests of individuals
- Examples:
 - Appropriate notice
 - User-friendly options
 - Rich privacy settings



Figure: “Tunnel Vision” by The 5th Ape, CC BY 2.0

Example: Amazon Alexa



Figure: “Amazon Echo Dot” by Mack Male, CC BY-SA 2.0

References I



Cavoukian, Ann (2012). "Privacy by design: origins, meaning, and prospects for assuring privacy and trust in the information era". In: *Privacy protection measures and technologies in business organizations: aspects and standards*. IGI Global, pp. 170–208.