



Rights by Design (RbD): Privacy Engineering for the Rights of All

Cat Easdon & Dr. Ryan Payne
18th Internet Governance Forum, Kyoto, Japan
10th October 2023



Who are we?



Cat Easdon

ECCRI European Cybersecurity Fellow;
Internet Society Early Career Fellow;
Privacy Engineer at Dynatrace



Dr. Ryan Payne

Researcher (Biometric Privacy) &
Lecturer at Queensland University of
Technology; Internet Society Early
Career Fellow

With thanks to:



All opinions expressed in this presentation are our own and do not necessarily represent the views of our affiliations.



Does Privacy Matter?

(Show of hands)



Should everything be private?



Availability of personal data enables our other rights

Think of the impact if your personal data isn't available:

- Travel abroad isn't possible (without proof of identity)
- No access to education / banking / asylum ... (without proof of identity)
- Employees can't be paid (without payroll data)
- Hospital patients can't be treated (without medical records)

Data wants to be available!



the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

Extract from Art. 32 GDPR security of processing

Other data protection legislation contains similar provisions, e.g. CPPA (California)

Privacy Defined

“An individual’s ability to withhold (or part) of thoughts, sentiments, emotions, and expressive works” - *Warren & Brandeis (1890) 198N.2*

Contextual Privacy (*Nissenbaum, 2009*)

- Privacy is provided by appropriate flows of information
- Appropriate information flows are those that conform with contextual information norms
- Contextual informational norms refer to five independent parameters: data subject, sender, recipient, information type, and transmission principle
- Conceptions of privacy are based on ethical concerns that evolve over time



Privacy and Our Rights



Individual Privacy Rights

- Right to know/access/export (+ portability: GDPR, LGPD)
- Right to rectify
- Right to be forgotten
- **Right to anonymity** (AfDec - AfIGF 2013, Kenya)
- Right not to be subject to automated decisions/profiling with legal effects (GDPR)
- Right not to be subject to real-time/remote biometric identification (EU AI Act + others)
- Plus rights from copyright, fraud, and defamation law (e.g. wrt. deep fakes, generative voice)

Privacy as an Enabling Right

“Privacy enables the enjoyment of other rights: the free development and expression of an **individual’s personality**, identity and beliefs, and their **ability to participate** in political, economic, social and cultural life.”

- UN Special Rapporteur on the right to privacy

Privacy as an Enabling Right

Digital privacy is a crucial enabler for:

- Freedom of expression, movement and assembly -> equal participation in society
- Freedom of thought and freedom from manipulation
- Autonomy and self-determination
- Non-discrimination
- An effective remedy and a fair trial
- Equality between women and men
- Internet access -> enabling access to education, medical advice, economic opportunities

Privacy as an Enabling Right



“Achieving the Sustainable Development Goals (SDGs) is not possible without bold action on human rights: more than 90% of the 169 SDG targets are related to human rights and labour standards”
- *UN Global Compact*



Case Study: Biometrics



Biometric Privacy



- **This includes physiological attributes:**
 - Facial Tracking
 - Fingerprints
 - Hand (Palm print)
 - Eye scan (Iris)

- **This can also include behavioural attributes:**
 - Speed of typing
 - Hand Signature
 - Voice
 - Walking Gait (way you walk)

Neurotech and Cognitive Liberty

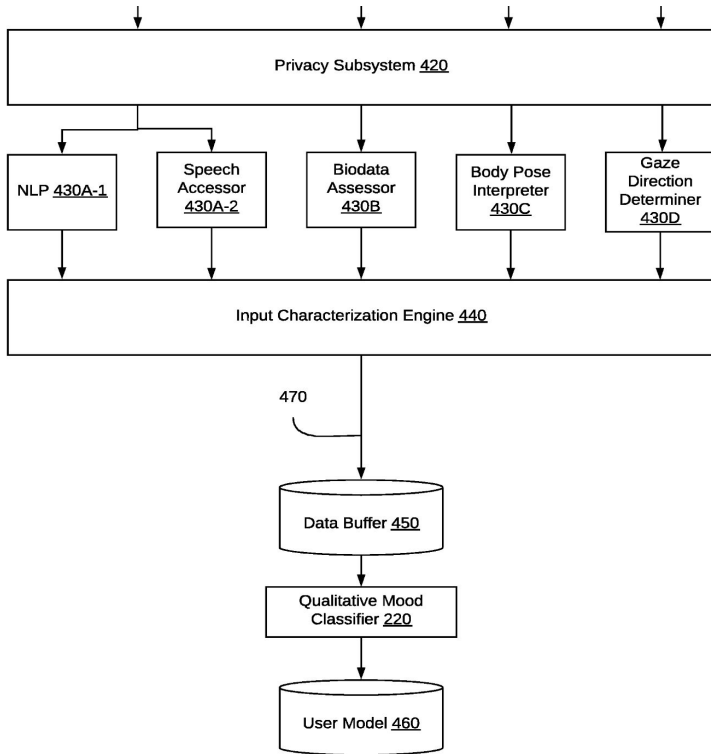


*“One of the coolest results involved **predicting a user was going to click on something before they actually did.** That was a ton of work and something I’m proud of. Your pupil reacts before you click in part because you expect something will happen after you click.*

So you can create biofeedback with a user's brain by monitoring their eye behavior, and redesigning the UI in real time to create more of this anticipatory pupil response.”

[Sterling Crispin](#) on his work at Apple as a Neurotechnology Prototyping Researcher

Neurotech and Cognitive Liberty



(12) **United States Patent**
Guerra Filho et al.

(54) **MODIFYING VIRTUAL CONTENT TO
INVOLVE A TARGET USER STATE**

(71) Applicant: **Apple Inc.**, Cupertino, CA (US)

*“the data processing architecture is configured to **obtain a request from the user to invoke a target state for the user** and generate, based on the user model ... CGR content intended to invoke the target state for the user. In some implementations, **the target state corresponds to an emotional state such as being scared, happy, sad, or the like.**”*

“physiological measurements of the user include at least one of eye tracking information, pupil dilation information, body pose characteristics, speech characteristics, heart rate, glucose level, and blood oximetry.”

Individuals' Collective Privacy

“Unique identifiable information is kept anonymous, but through data aggregation, collective group behaviours create archetypes of behaviours that an ‘unknown individual’ can be slotted into by algorithms to personally target them.”

Payne, R., Martin, B. A., Tuzovic, S., & Wang, S. (2023).
Defining Biometrics With Privacy and Benefits:
A Research Agenda for Academics and Public Policy Makers.
Australasian Marketing Journal, 14413582231167645.





Privacy Engineering and PbD (Privacy by Design)



What is Privacy Engineering?

1

An act of translation:

- From **law and policy** into **code**
- From the **social and political** realm into the **digital**

2

Where **software**, the **law**, and **ethics** meet, with the aim of ensuring that everyone has their rights respected and their data processed fairly.

3

IAPP: applying **systematic, scientific or methodological approaches** to include requirements for privacy in **design, development, and operations** in:

- Software development
- Data science
- System design
- Process design
- IT infrastructure
- Human-computer interaction and user experience design
- Physical architecture

Privacy Architecture - Physical Edition

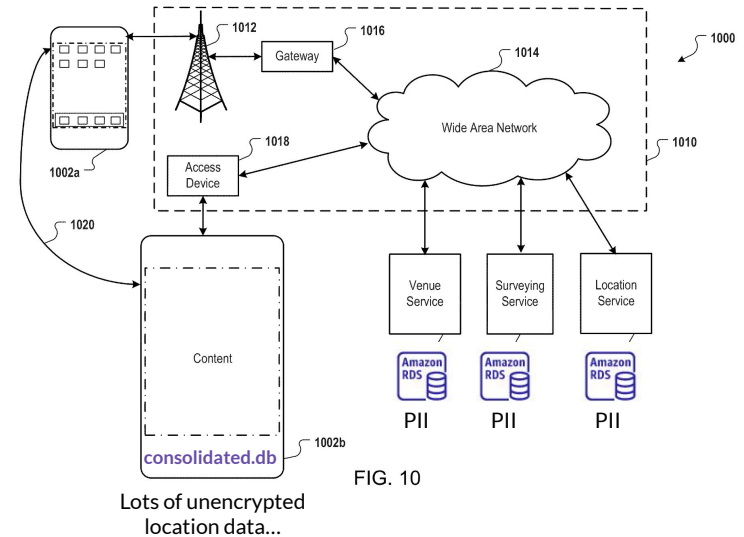


Image attribution, left to right: [E. Perales](#), [Noel Reynolds](#), [Masakazu Matsumoto](#). Used from Flickr under CC BY 2.0.

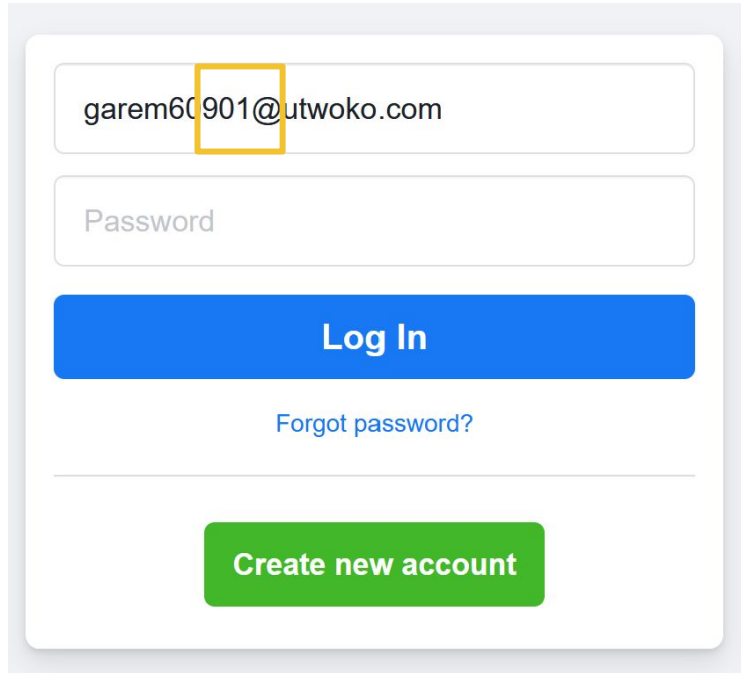
Privacy Architecture - Digital Edition

Software development practices and the pace of change have provided benefits for us - but have also created many privacy challenges:

- *“We didn’t implement deletion”*
- *“We might have that data, but I have no idea where”*
- *“I can’t remember what this database is used for. Mike built this, but he left the company. Some system is still updating it each day, we’d better not delete it”*



Privacy Architecture - Digital Edition



garem60901@utwoko.com

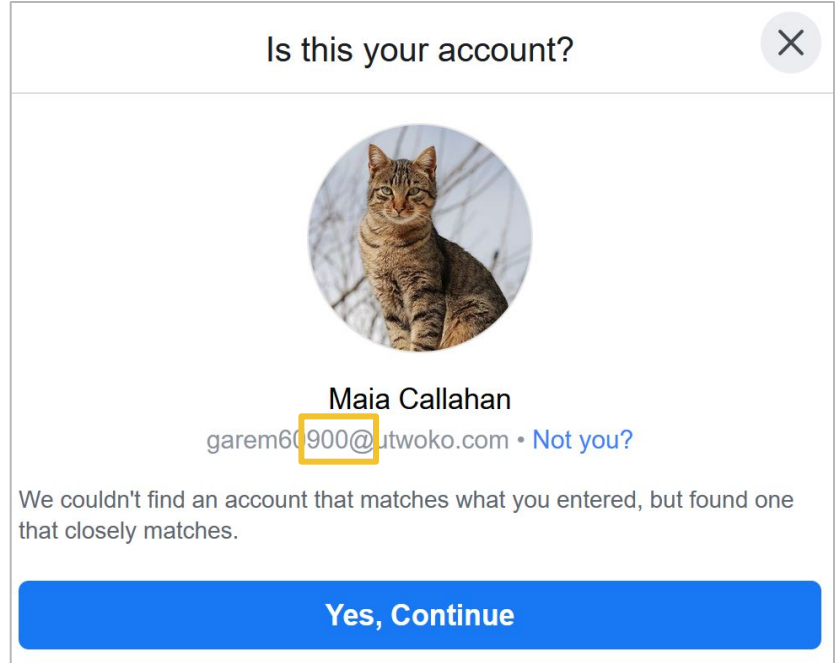
Password

Log In


[Forgot password?](#)

Create new account

The image shows a login form with a white background and rounded corners. The email input field contains 'garem60901@utwoko.com' and is highlighted with a yellow border. Below it is a password input field with the placeholder text 'Password'. A blue button labeled 'Log In' is centered below the fields. Underneath the button is a link for 'Forgot password?'. At the bottom of the form is a green button labeled 'Create new account'.



Is this your account?



Maia Callahan
garem60900@utwoko.com • [Not you?](#)

We couldn't find an account that matches what you entered, but found one that closely matches.

Yes, Continue

The image shows a modal dialog box with a white background and rounded corners. At the top, it asks 'Is this your account?' with a close button (X) in the top right corner. Below the text is a circular profile picture of a brown tabby cat. Underneath the picture, the name 'Maia Callahan' is displayed in bold, followed by the email 'garem60900@utwoko.com' and a link 'Not you?'. The email field is highlighted with a yellow border. Below this information is a message: 'We couldn't find an account that matches what you entered, but found one that closely matches.' At the bottom of the dialog is a blue button labeled 'Yes, Continue'.

Screenshots of <https://www.facebook.com/> illustrating a privacy-usability tradeoff in the login UI. Such design decisions are challenging to make because different users' needs and privacy expectations vary widely.

Privacy by Design (PbD)

- Proactive not reactive; preventive not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality - positive-sum, not zero-sum
- End-to-end security - full lifecycle protection
- Visibility and transparency - keep it open
- Respect for user privacy – keep it user-centric

From *Privacy by Design: The 7 Foundational Principles* by Ann Cavoukian

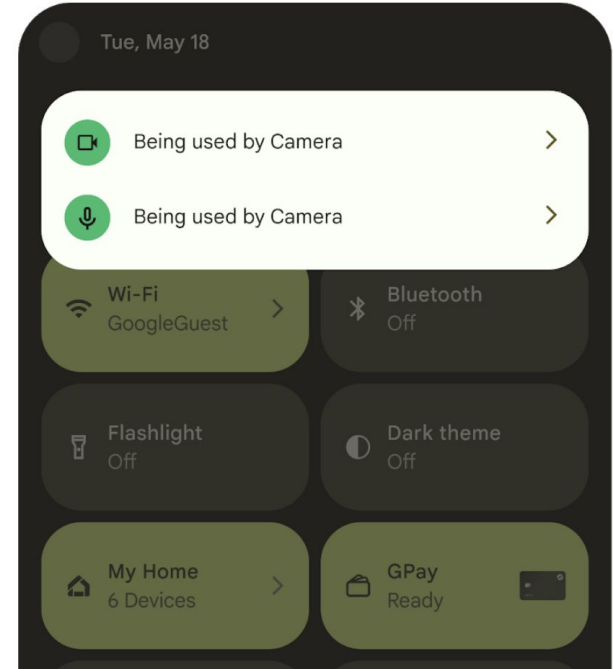


Image reproduced from work created and [shared by the Android Open Source Project](#) and used according to the [Creative Commons 3.0 Attribution License](#).

Rights by Design (RbD)

- Privacy enables many of our other rights, so when threat modeling for privacy by design, we need to expand our thinking far beyond privacy and implement **rights by design**.
- If I process this data about my users: how might their rights be violated? What are the worst-case scenarios? How could I prevent them?
 - Data requested by law enforcement to enforce unethical law -> user sent to prison or sentenced to death
 - User's stalker / abusive spouse learns their location -> physical abuse or murder
 - User's network metadata looks suspicious -> targeted assassination by drone

But how could [insert product here] violate anyone's rights?



Adapted from Privacy Harms, Citron & Solove, Boston University Law Review (2022)



Applying Rights by Design



Applying RbD: Businesses

“Businesses should support and respect the protection of internationally proclaimed human rights; and make sure that they are not complicit in human rights abuses”
- UN Global Compact

Ensure your products are grounded in ethical principles that respect human diversity:

- This starts with providing ethics and threat modeling training (LINDDUN, PLOT4AI, Microsoft Harms Modeling) to build an ethical culture
- Establish an ethical code of conduct - what will you refuse to build?
- Design potential for human intervention into AI systems and conduct regular fairness and bias testing

Applying RbD: Businesses

Category	Type of Harm	Severity	Scale	Probability	Frequency	Overall Potential
Risk of injury	Physical or infrastructure damage	Low
	Emotional or psychological distress	Low
Denial of consequential services	Opportunity loss	Medium
	Economic loss	Low
Human rights infringement	Dignity loss	Low
	Liberty loss	Low
	Privacy loss	High
	Environmental impact	Medium
Erosion of social and democratic structures	Manipulation	Medium
	Social detriment	Medium

Source: Microsoft Harms Modeling Framework

Applying RbD: Policymaking

- UN Convention on Cybercrime
 - Crucial that the treaty contains explicit human rights protections
 - Proposed “cyber-enabled crimes” must be proportionate and not an attempt to bypass human rights protections
- UK Online Safety Bill, EU CSAM Regulation, and other attacks on encryption
 - There is no “safe”, privacy-preserving way to backdoor encryption
 - Be sceptical of any appeals to emotion in policy (child safety, terrorism, etc). It’s not about safety, but about exploiting fear to consolidate power

Discussion Questions

1. How should we govern AI to protect privacy?
2. How could you apply Rights by Design in your work?
3. Where do you see potential to apply Rights by Design to tech policymaking?

Thank you.

If you'd like to learn more, we invite you to check out Ryan's research and Cat's free online course: *Introduction to Privacy Engineering*.

