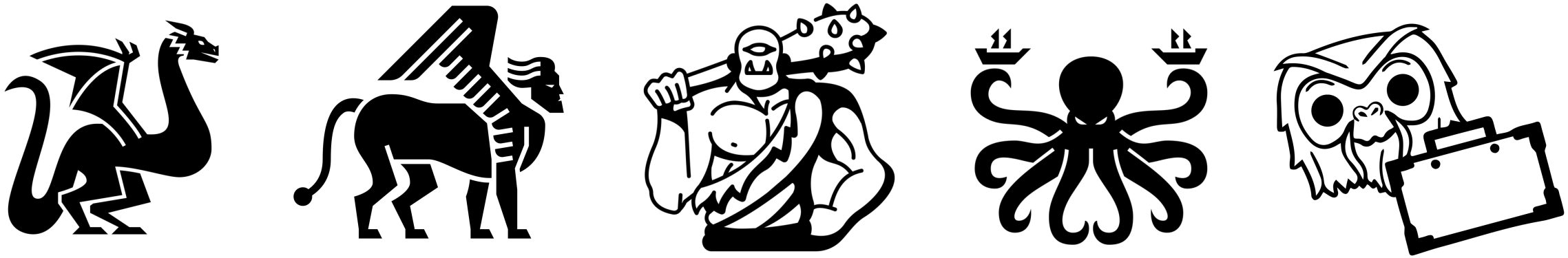
iapp

Fantastic Privacy Threats and Where to Find Them

"The amusing creatures described hereafter are fictional and cannot hurt you." ~ Albus Dumbledore



Cat Easdon - Privacy Auror 🪄 🧙‍♀️ at Dynatrace

Outline

- Why care about privacy threats?
- How do we threat model?
- Tour of privacy threats

Before we begin

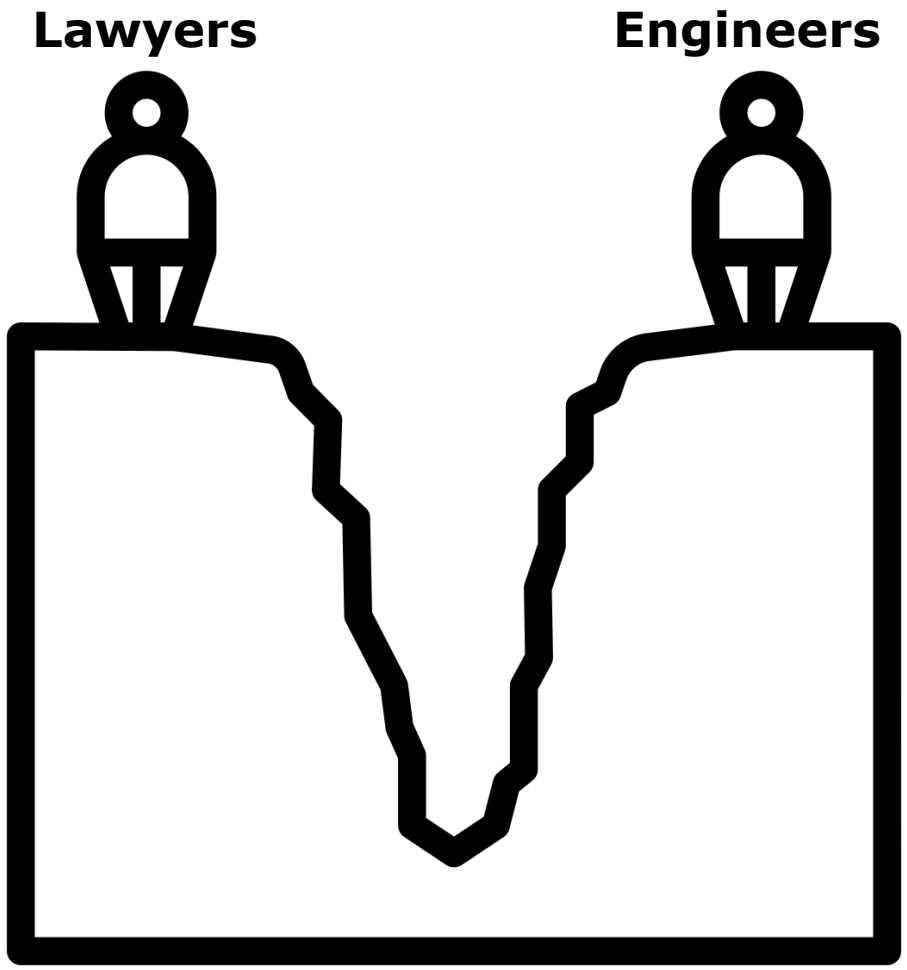
All our discussion beyond the slides today is under the Chatham House rule:

- Use what you learn in your work (that's the whole point…)
- But don't reveal directly or indirectly who said what



Intro

An unbridgeable chasm?



An unbridgeable chasm?



ANALYSIS

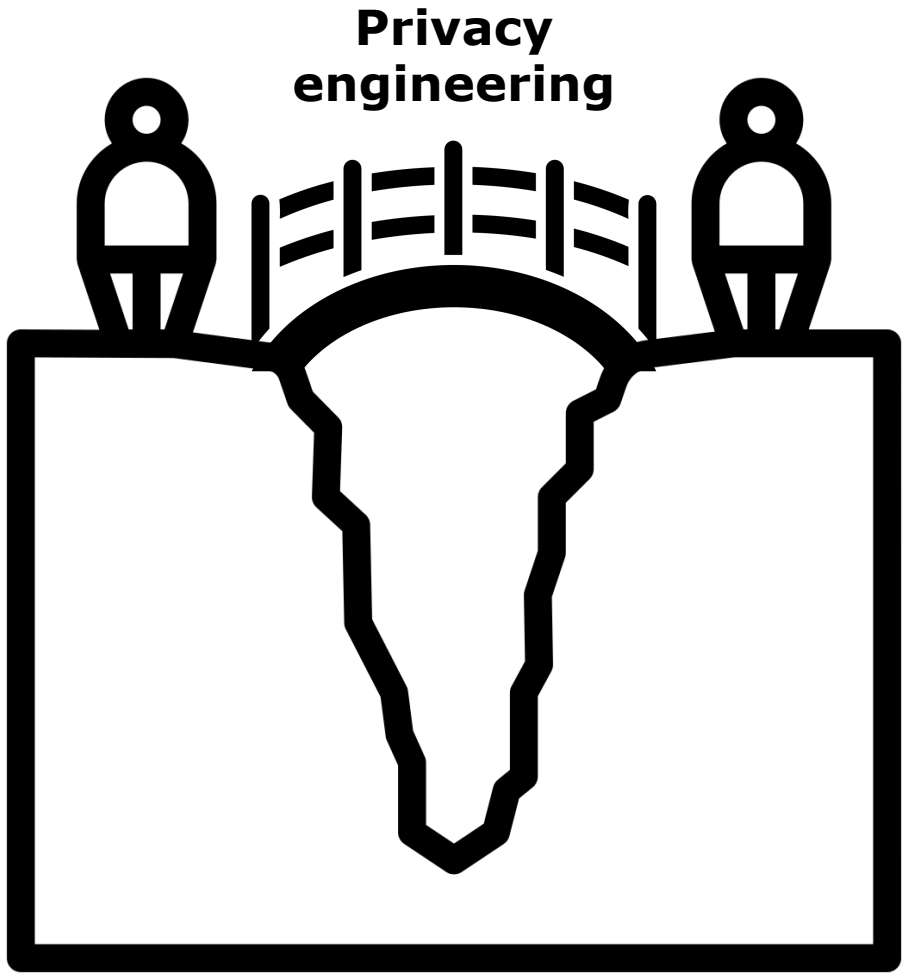
iapp

Engineers and Lawyers in Privacy Protection: Can We All Just Get Along?

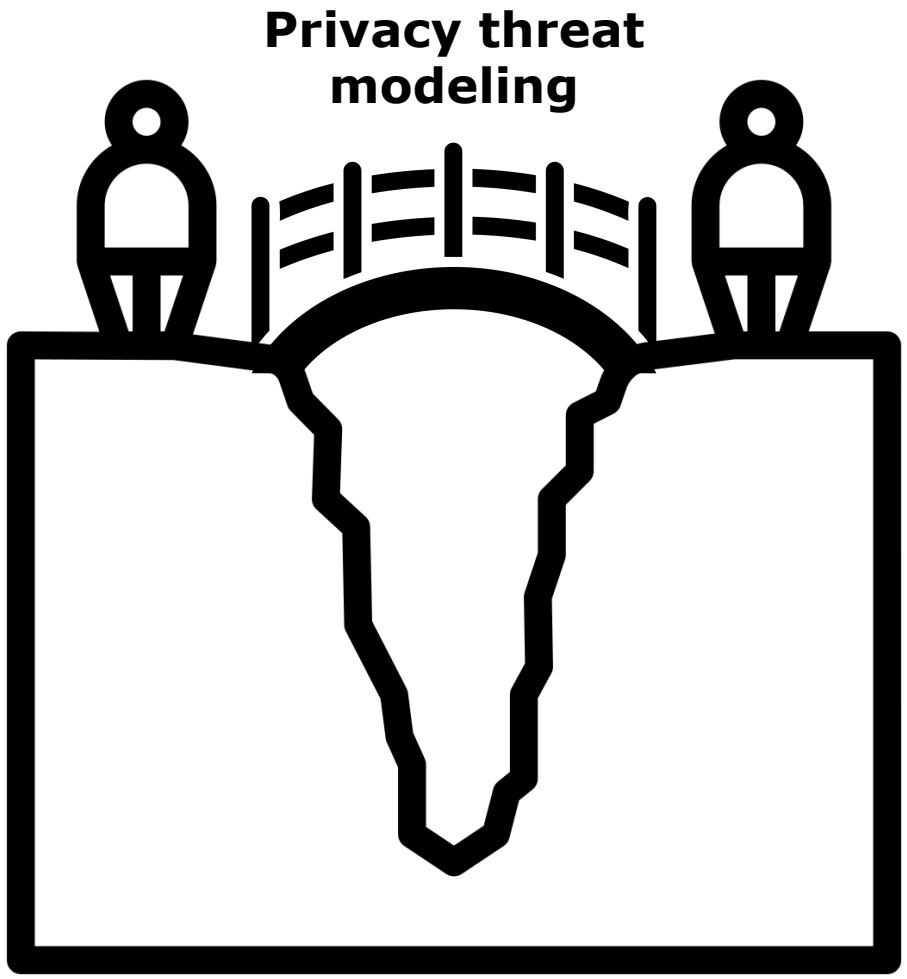
Published
13 Jan. 2014

Subscribe to IAPP newsletters →

Privacy engineering as bridge



Today: privacy threat modeling as bridge



What is threat modeling?

CNIL. *PIA, methodology* June 2015 Edition

3. Risks: potential privacy breaches

Objective: gain a good understanding of the causes and consequences of risks.

Step	Description	Report
		❑ Risk map ❑ Detailed description of the risks

What is threat modeling?



1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

Why threat model?

iapp

Impact assessments

- GDPR: **data protection impact assessment** (DPIA) required if a new processing activity is likely to result in high risk
  - Also known as a **privacy impact assessment** (PIA)
- Common in risk-based digital regulation, e.g. the AI Act's **fundamental rights impact assessment** (FRIA)



Why threat model?

Understanding risks to rights and freedoms is also essential to:

- Determine whether legitimate interest is a valid legal basis for processing (Article 6)
- Determine appropriate technical and organizational measures for data protection by design and default (Article 25) and for security (Article 32)
- Decide whether notification to the SA and communication to data subjects is required for a personal data breach (Articles 33-34)
- …

Why threat model?

And this risk assessment is hard! Especially because the SA and EDPB examples tend to be the obvious ones:

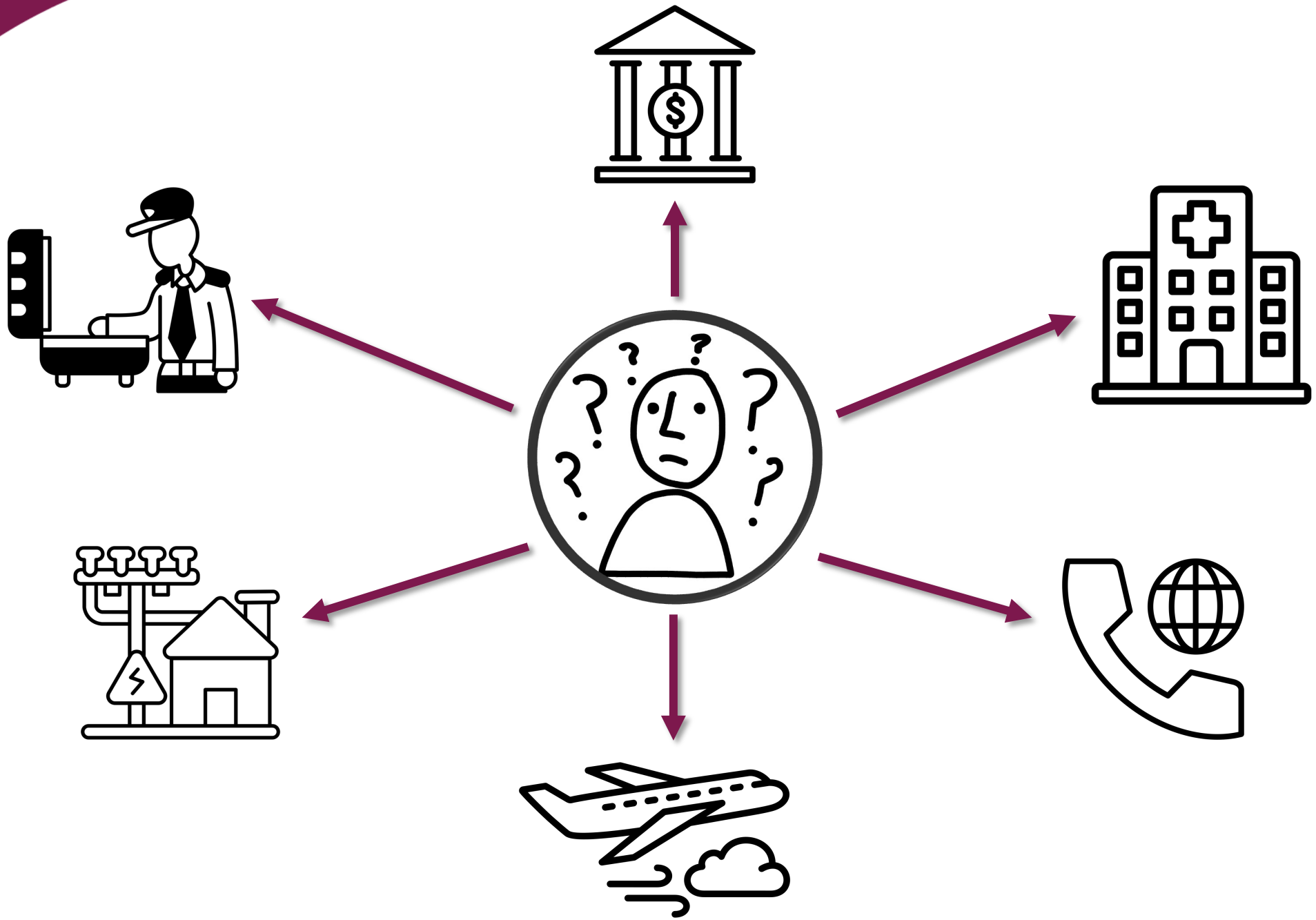
- Obviously a new project processing the location data of every citizen of a country or children's biometric data is high risk and needs your attention…
- But what about 'normal' stuff?
  1. Yet another new AI tool company-wide
  2. IT want to buy some new software
  3. Marketing want to put some videos on the website

How do we threat model?

~~Creative writing~~ Threat modeling for beginners

Start as if you were writing a story…

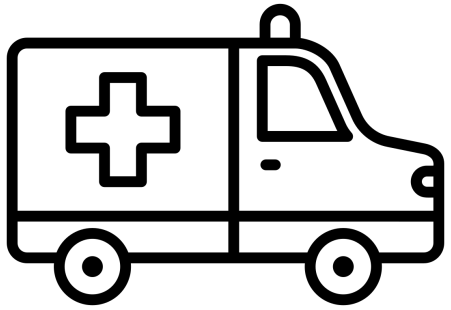
- Who is your data subject?
- When do they use the product/service? Where are they when they use it?
- What's their goal?
- Are they under pressure? Who or what are they afraid of?
- Which details about themselves do they consider sensitive in this context?

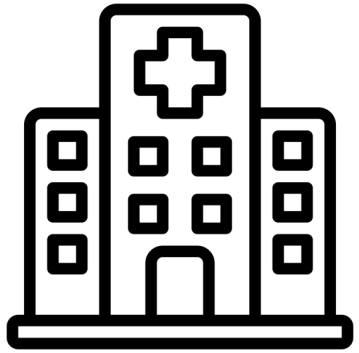


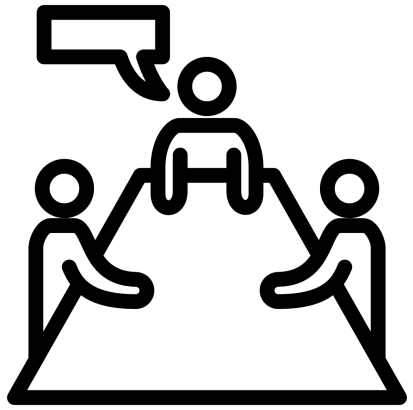
~~Creative writing~~ Threat modeling for beginners

While writing your “story”, consider which information flows are appropriate in this context:

- Consider data type, data subject, sender, recipient, legal basis, purpose



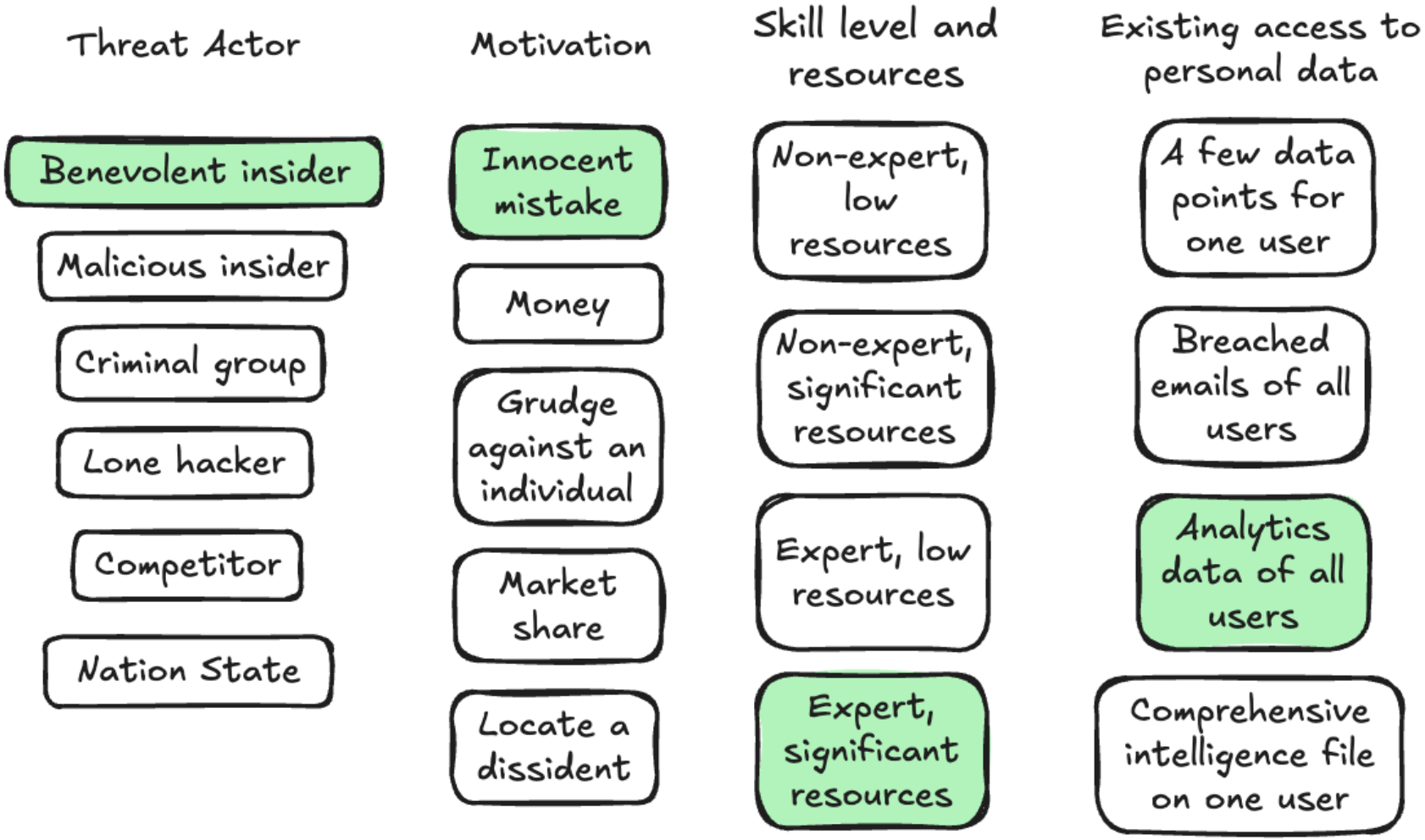




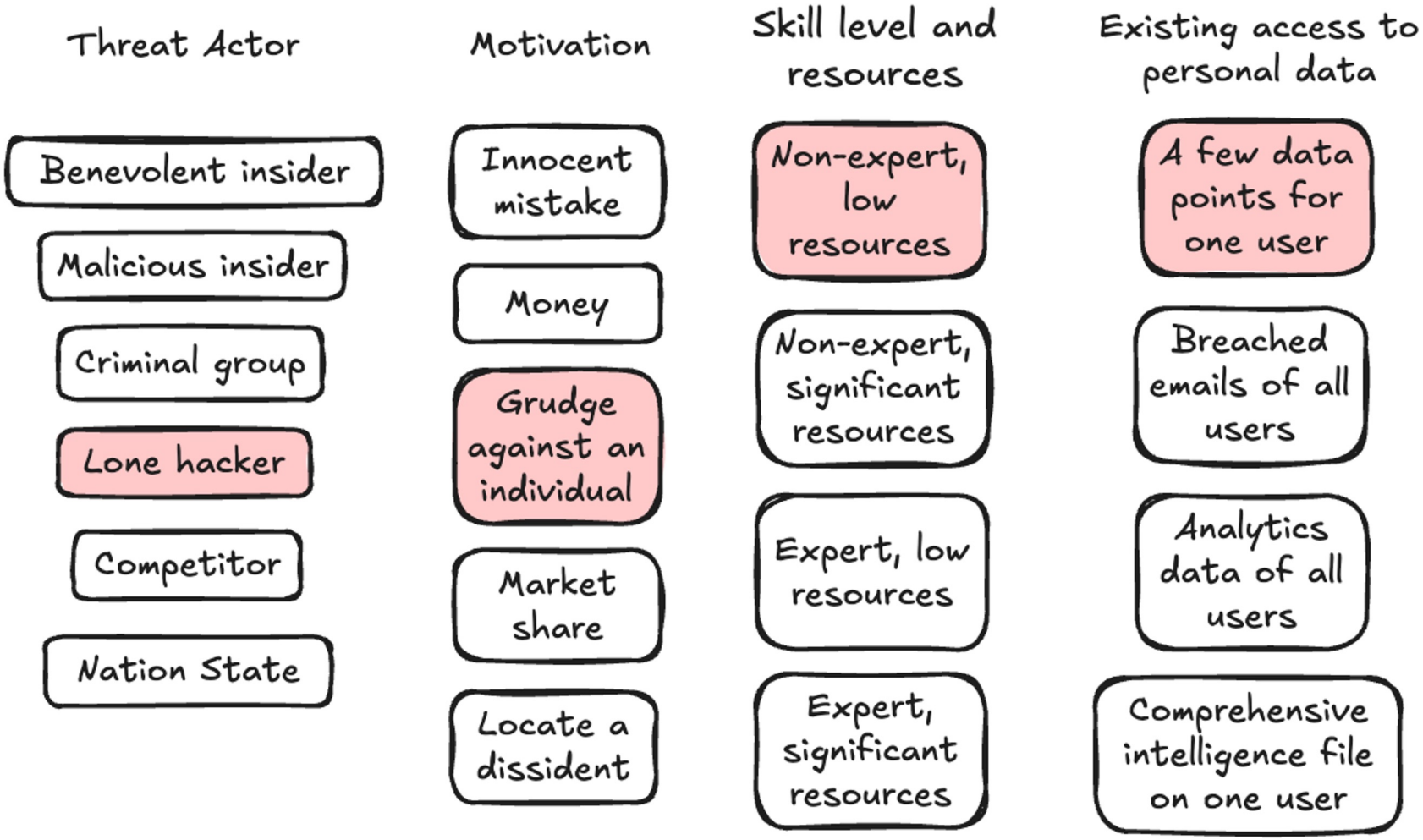
Personas



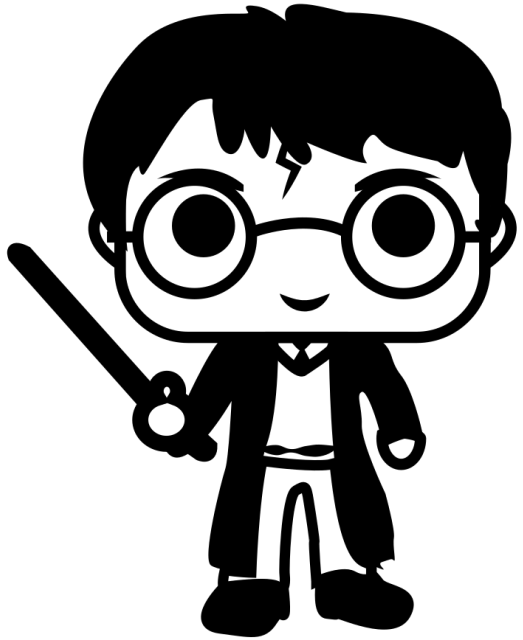
Threat actor personas



Threat actor personas



User personas





User personas

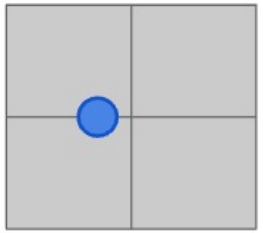
Created by the Open Internet Tools Project – see [User Personas for Privacy and Security](#) by Gus Andrews



Shura

"Help me remain unknown, yet still be a visible leader."

- Mid-20s gay man
- Urban Russia
- Blogger/publisher
- Lives with a bunch of roommates
- Excited by the work he does; sometimes a little too bold for his safety



Technology expertise level
- Social media savvy
- Less smart about operational security

Technology use
- Mobile all the way
- Blogs but doesn't run own server
- Participant in online groups
- Cavalier about posting and privacy settings
- Uses desktop software less often

Access locations
- Anywhere there's connectivity

Threats from technology use
- Lose day job due to being "outed" by thugs researching his activity on social media

Physical threats
- Beating or death
- Jail for activism around LGBT issues

Needs
- To remain anonymous BUT wants his pseudonym to be well-known
- Wants to communicate to a lot more people
- Find places to meet in public

Security: STRIDE













Privacy: LINDDUN









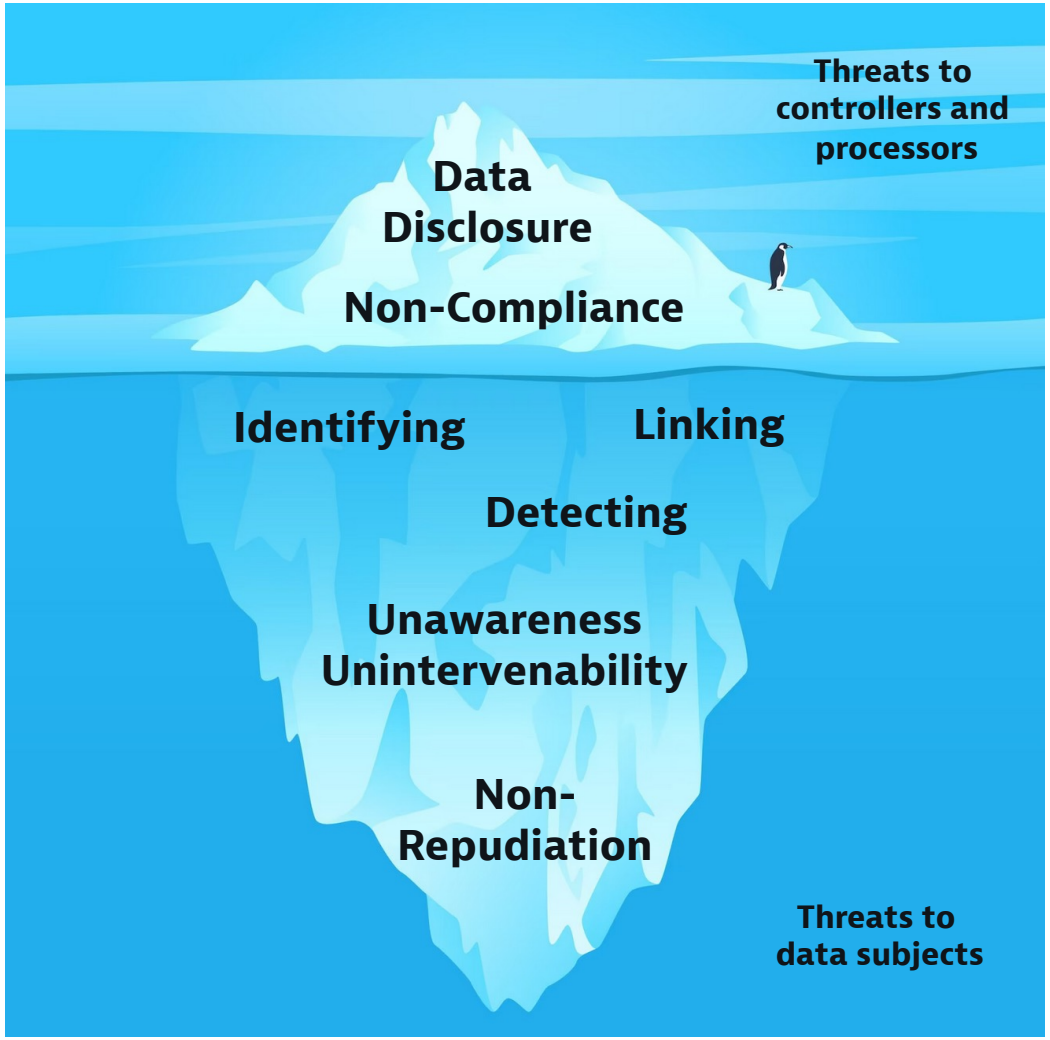






Privacy: LINDDUN

Image designed by Freepik



Privacy threats cause harms

User #15978623's ad profile

General attitudes - I generally get a raw deal out of life

Health - Addictions - Alcohol

Demographics - Marital Status - Likely Recently Divorced

Interest - Entertainment - Party and Night Club Enthusiasts

Alcoholic Drinks - Vodka - Grey Goose for age 21+ - Likely

Source: The Markup (2023). Segment names have been adapted to remove names of data brokers.

Privacy threats cause harms

Privacy Threat
Linkability
Identifiability
Non-Repudiation
Detectability
Data Disclosure
Unawareness, Unintervenability
Non-Compliance

Privacy Harms
Physical Harms
Economic Harms
Reputational Harms
Autonomy Harms
Psychological Harms
Discrimination Harms
Relationship Harms
Harm to the Business

Autonomy Harms
Coercion
Manipulation
Failure to Inform
Thwarted Expectations
Lack of Control
Chilling Effects

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

Complete threat model: outline

1. Metadata *(last updated at … by …, update when project … begins)*
2. System description *including intended use cases (!!)*
3. Table of personal and customer data types processed
   - With risk reasoning and data subject rights info (can it be updated, exported, deleted?)
4. Table of data sources and sinks with geolocation
5. Supplementary data flow diagrams
6. Internal access to data
7. Customer control over data and transparency
8. Identified threats grouped by NIST Privacy Triad category *(predictability, manageability, disassociability)*

A little tour of privacy threats

Before we begin

Ministry of Magic (M.O.M.) classifications of ~~beasts~~ privacy threats:

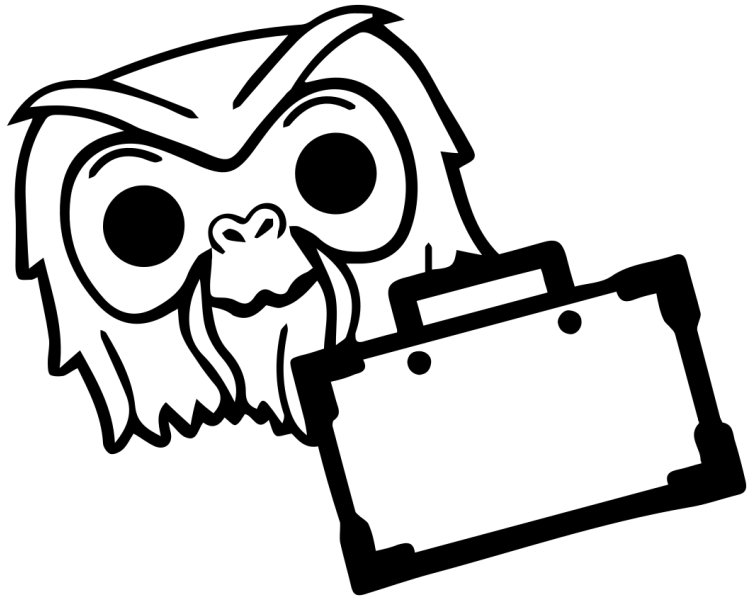
- X: Boring
- XX: Harmless, may be domesticated
- XXX: Competent ~~wizard~~ privacy auror should cope
- XXXX: Dangerous, require specialist knowledge
- XXXXX: Known ~~wizard~~ privacy auror killer, impossible to train or domesticate. Basically anything that Hagrid likes, or that the *SA-that-shall-not-be-named* might open a 5-year inconclusive inquiry about.

Unofficial:

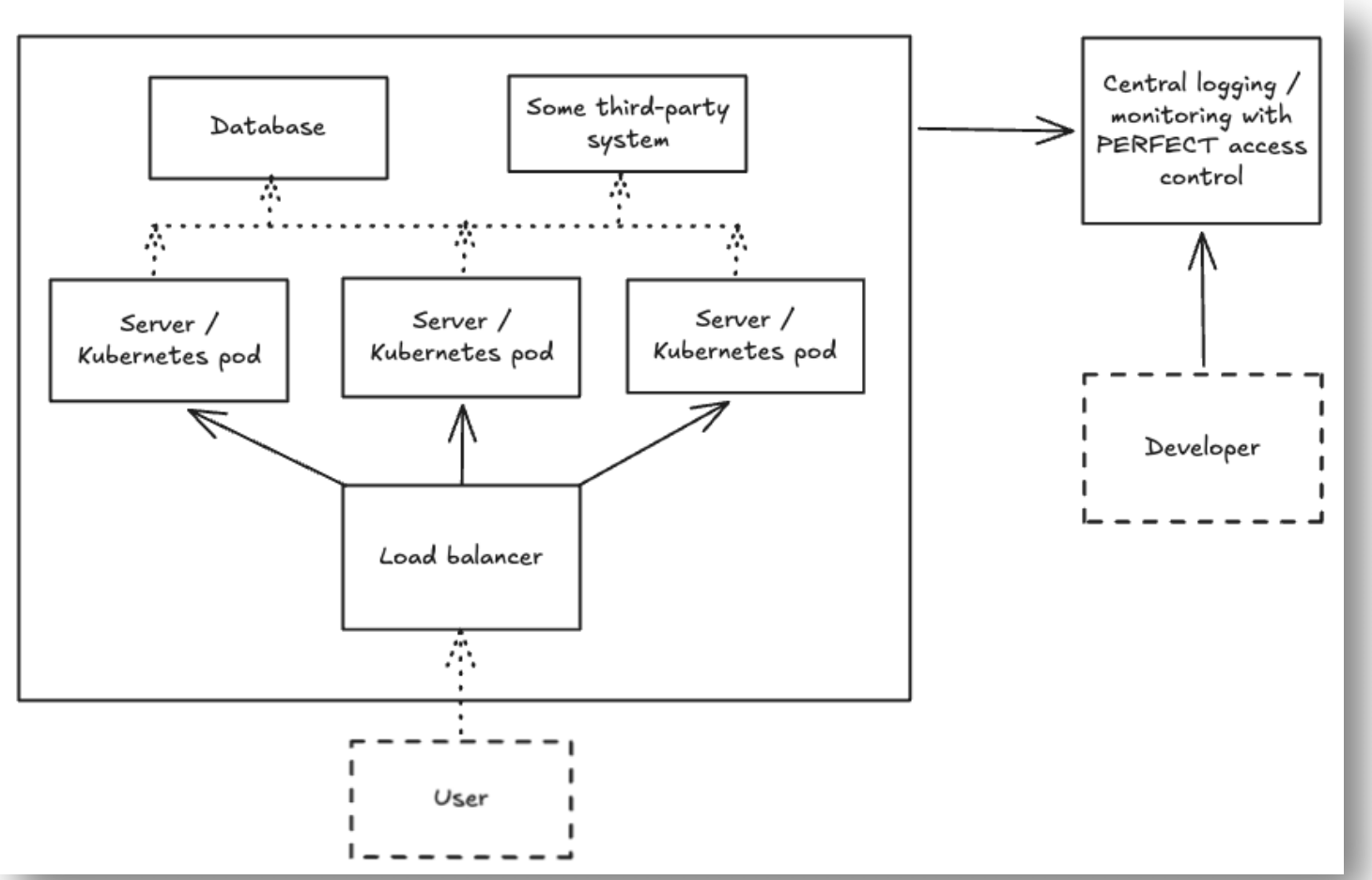
- XXXXXXX: Pixies, if you're Professor Lockhart
- XXXXXXXXX: Aragog, according to Ron 

Illusory access control (Securitas theatrum)

Natural habitat: complex software systems
M.O.M. Classification: XXXX
LINDDUN: data disclosure
Notable (dark) magical uses: troubleshooting, repurposing data
Data diet: EVERYTHING

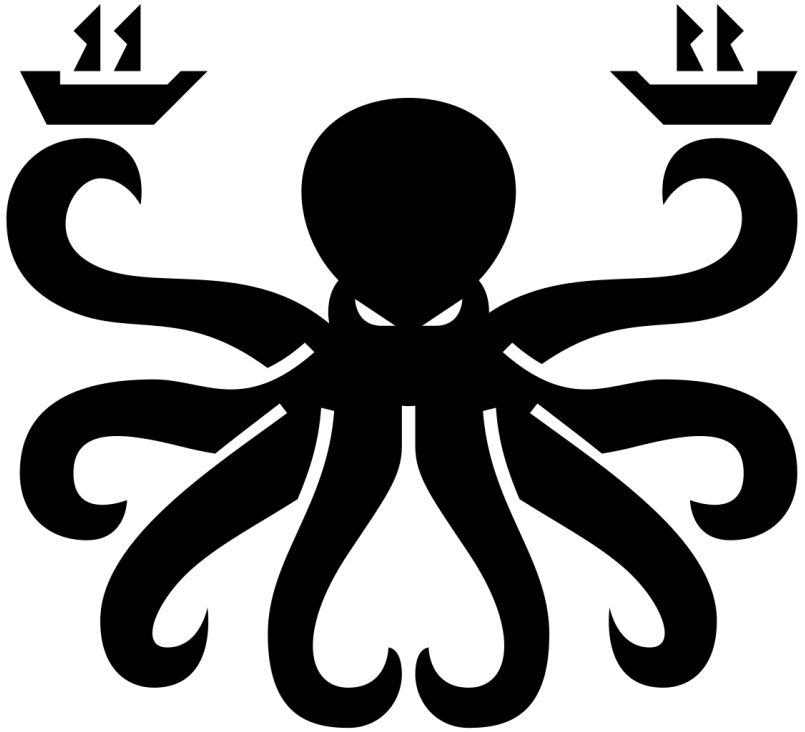


Illusory access control (Securitas theatrum)

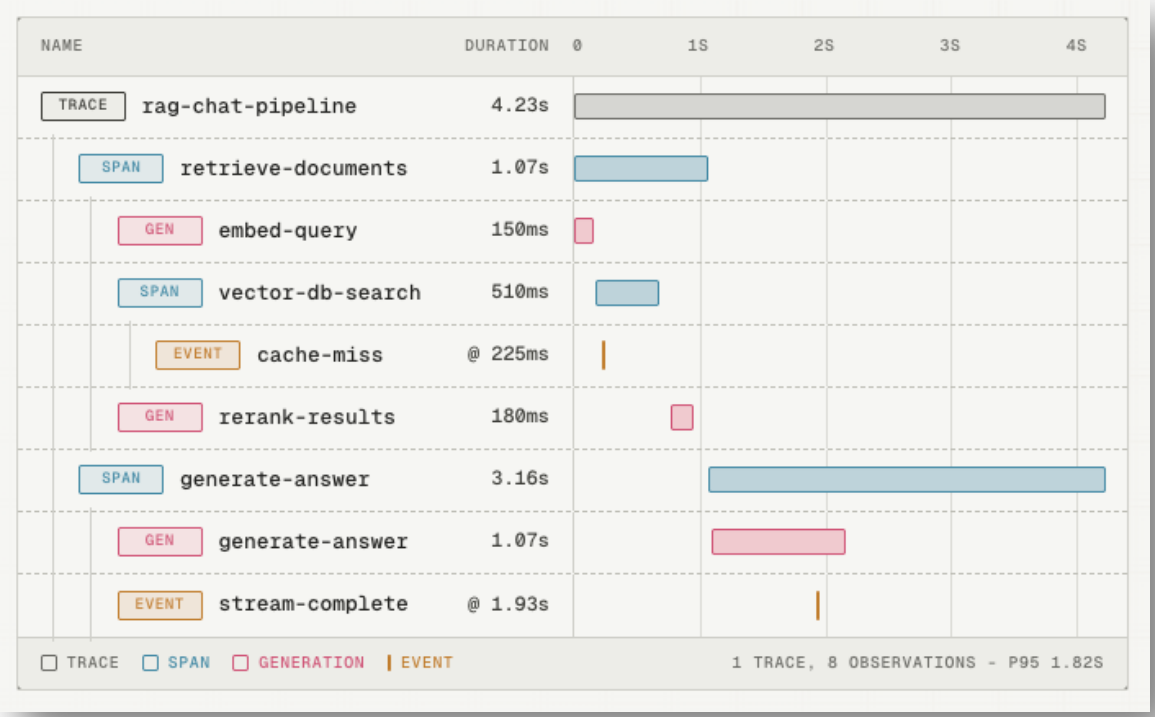


Misconfigured logging and telemetry (Dashboardus Maximus)

Natural habitat: complex software systems
M.O.M. Classification: XXX
LINDDUN: data disclosure
Notable (dark) magical uses: troubleshooting, business automation
Data diet: much more than just technical details



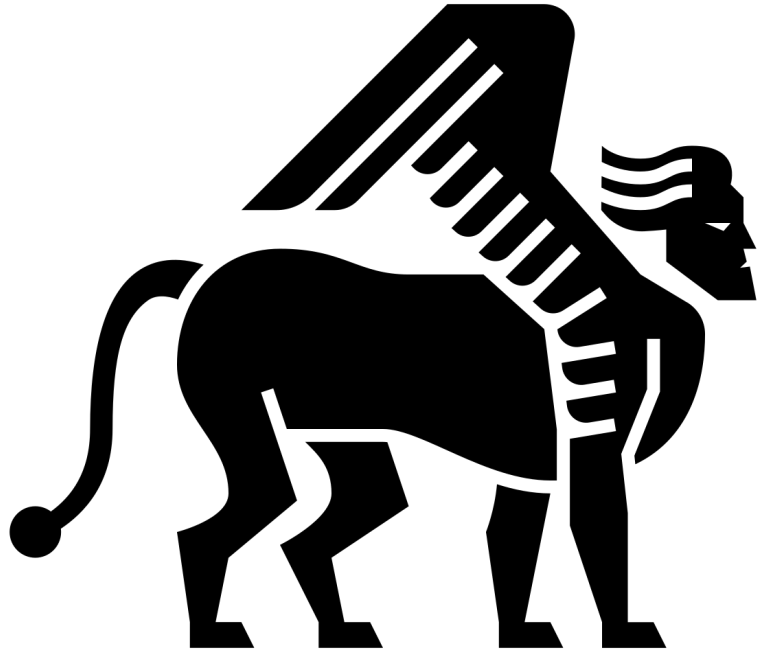
Misconfigured logging and telemetry (Dashboardus Maximus)



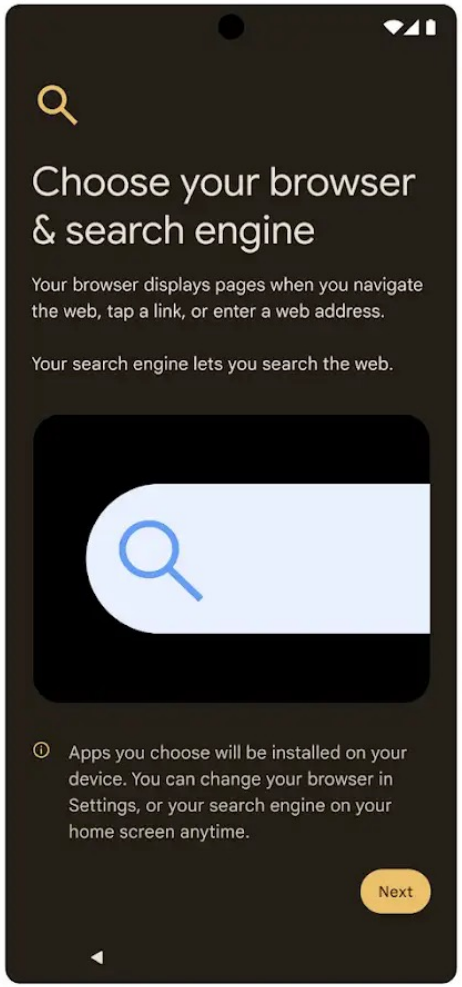

```
Session: conversation_8f2a
├── Trace: "Why was I charged twice this month?"
├── Trace: "Can you refund the duplicate?"
└── Trace: "Thanks, when will I see it?"
```

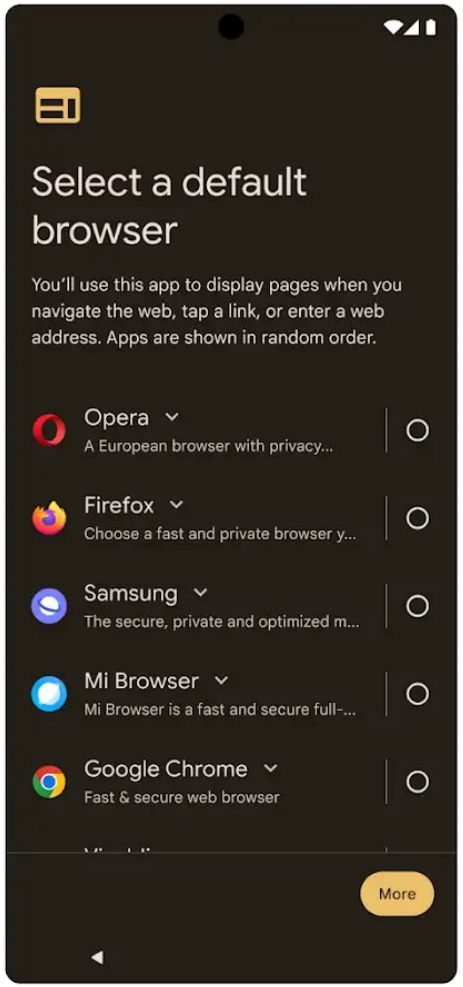
Cryptic privacy choices (Libertas illusoria)

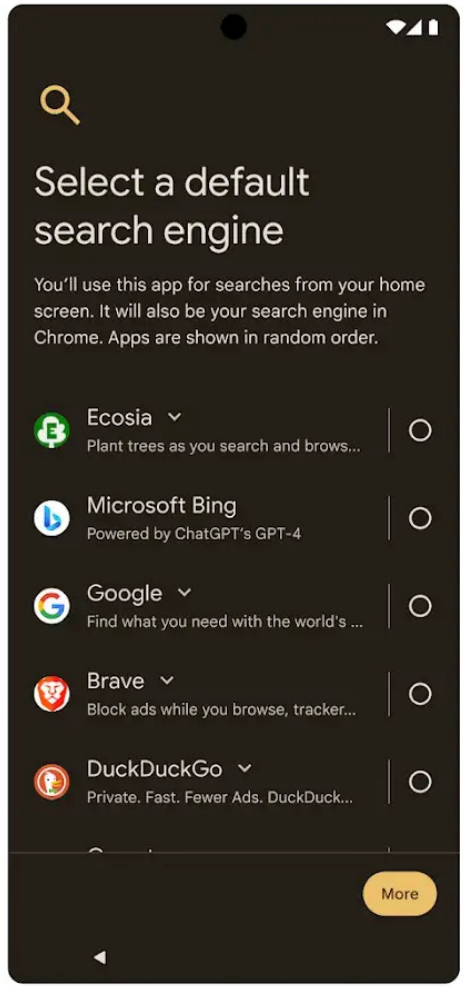
Natural habitat: any user-facing interface or communication
M.O.M. Classification: XXXX
LINDDUN: unawareness & unintervenability
Notable (dark) magical uses: cookie dialogs, settings, defaults
Data diet: user info



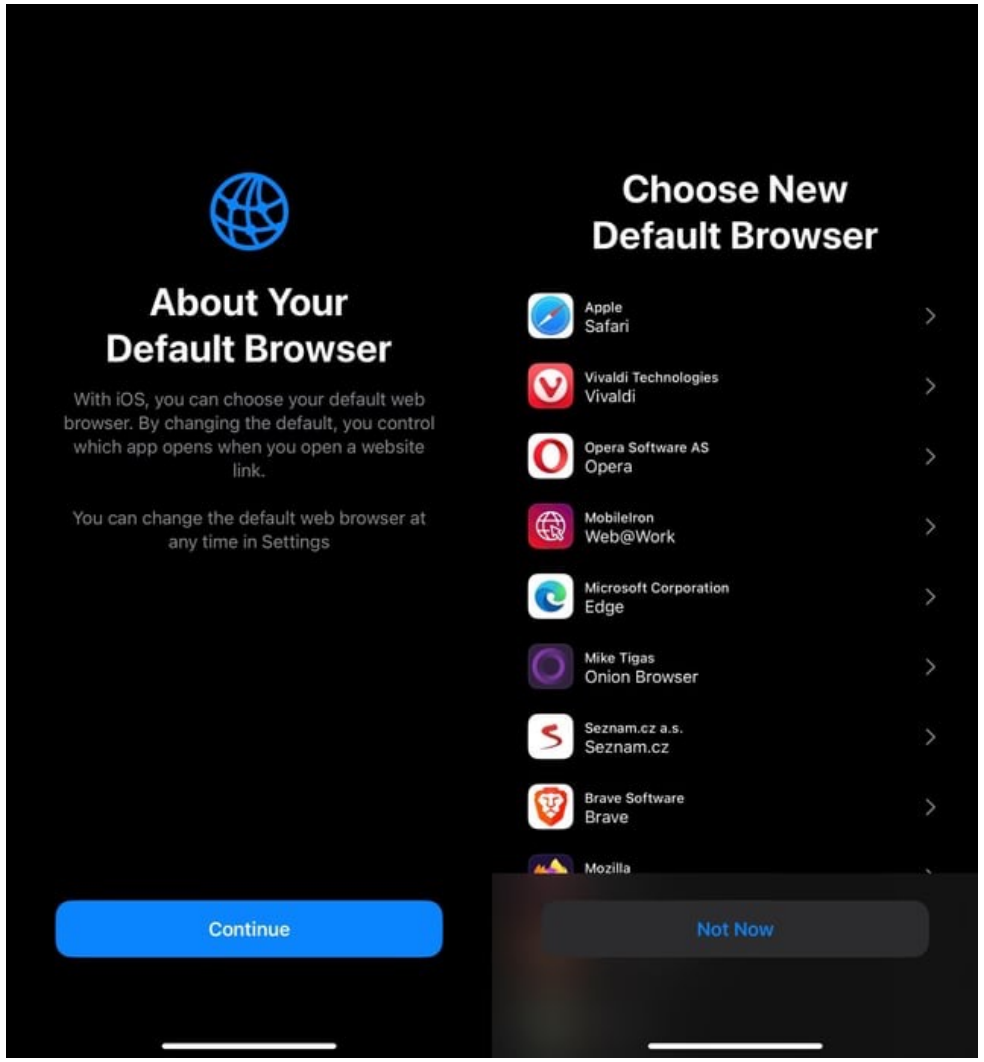
Cryptic privacy choices (Libertas illusoria)







Cryptic privacy choices (Libertas illusoria)

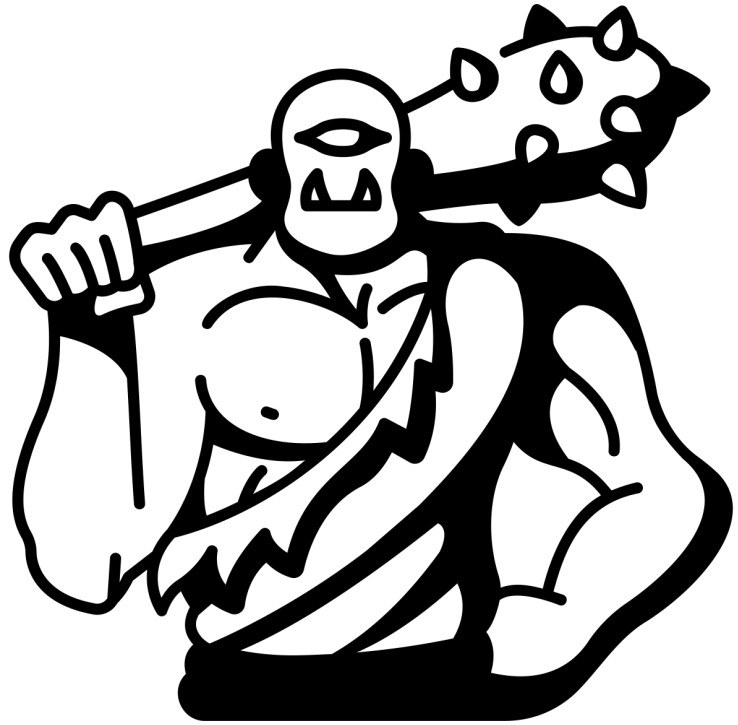


Cryptic privacy choices (Libertas illusoria)

We asked people what they think happens after they choose a default browser. **Only about half (52%) of people understand that their default browser is opened when they, for example, click on a link in an email or document.**[60] This share did not significantly vary across treatment groups, which is surprising as the Q&A screen (displayed to T2-4) explicitly states this is what happens when they select a default browser. Moreover, 6% of people incorrectly believe that they are *only* able to use their default browser (i.e., that all other browsers would be disabled). Even more significantly, **over half (53%) also erroneously believed that their default browser would automatically be pinned to their taskbar.** Previous research suggests this is a common misconception - and the impact of not being pinned to the taskbar, in terms of how this impacts people's usage of browsers, is an area where we consider further research could be undertaken.

Assumed cultural context (Contextus praesumptus)

Natural habitat: multinational orgs, social media platforms
M.O.M. Classification: XXX
LINDDUN: unawareness & unintervenability
Notable (dark) magical uses: user interfaces, settings and defaults
Data diet: user info



Assumed cultural context (Contextus praesumptus)



About Design DIS 2016, June 4–8, 2016, Brisbane, Australia

Privacy & Social Media in the Context of the Arab Gulf

Norah Abokhodair*
University of Washington
Seattle, USA
noraha@uw.edu

Sarah Vieweg
Qatar Computing Research Institute
Doha, Qatar
svieweg@qf.org.qa

"As Saudis we know how to keep our private life private and what is suppose to be public, we still keep private." First author: *"Like what?"* M5: *"Your name, your work, your mother's name…the worst example we have here…a lot of guys are ashamed of their mothers' name."*

Assumed cultural context (Contextus praesumptus)



About Design

DIS 2016, June 4–8, 2016, Brisbane, Australia

Privacy & Social Media in the Context of the Arab Gulf

Norah Abokhodair*
University of Washington
Seattle, USA
noraha@uw.edu

Sarah Vieweg
Qatar Computing Research Institute
Doha, Qatar
svieweg@qf.org.qa

"Four years ago when Facebook changed the privacy settings, one of my friends liked a picture of my family, the picture had my sister in it, and I got really upset and embarrassed that he could see that picture of my sister in it, so I deactivated my account for about six months, I think."

Assumed cultural context (Contextus praesumptus)



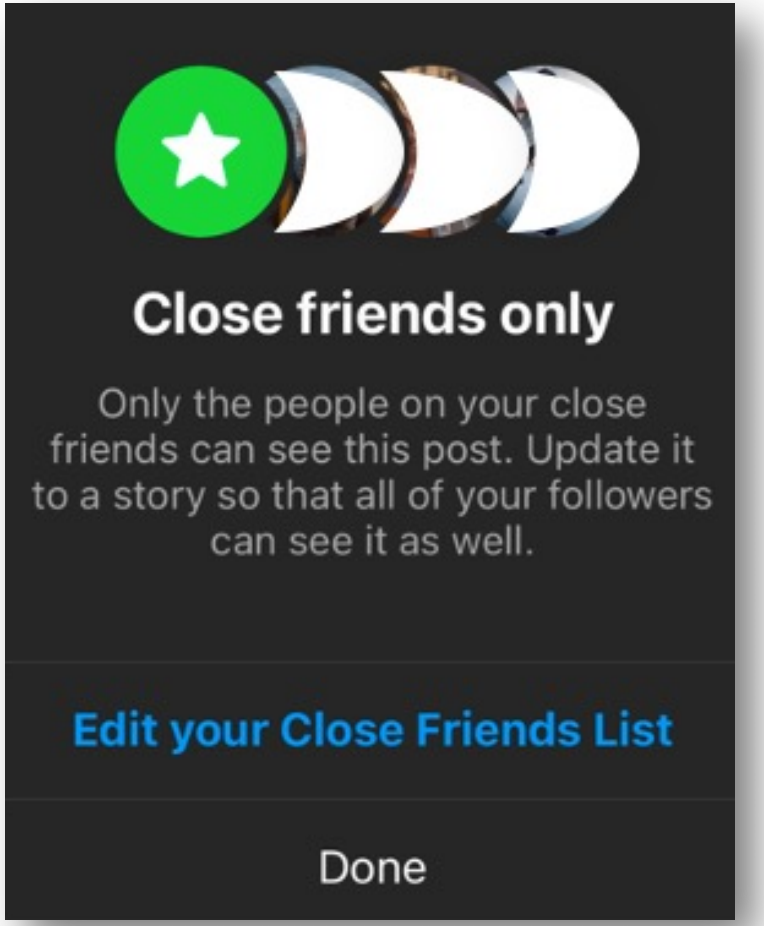
Privacy & Social Media in the Context of the Arab Gulf

Norah Abokhodair*
University of Washington
Seattle, USA
noraha@uw.edu

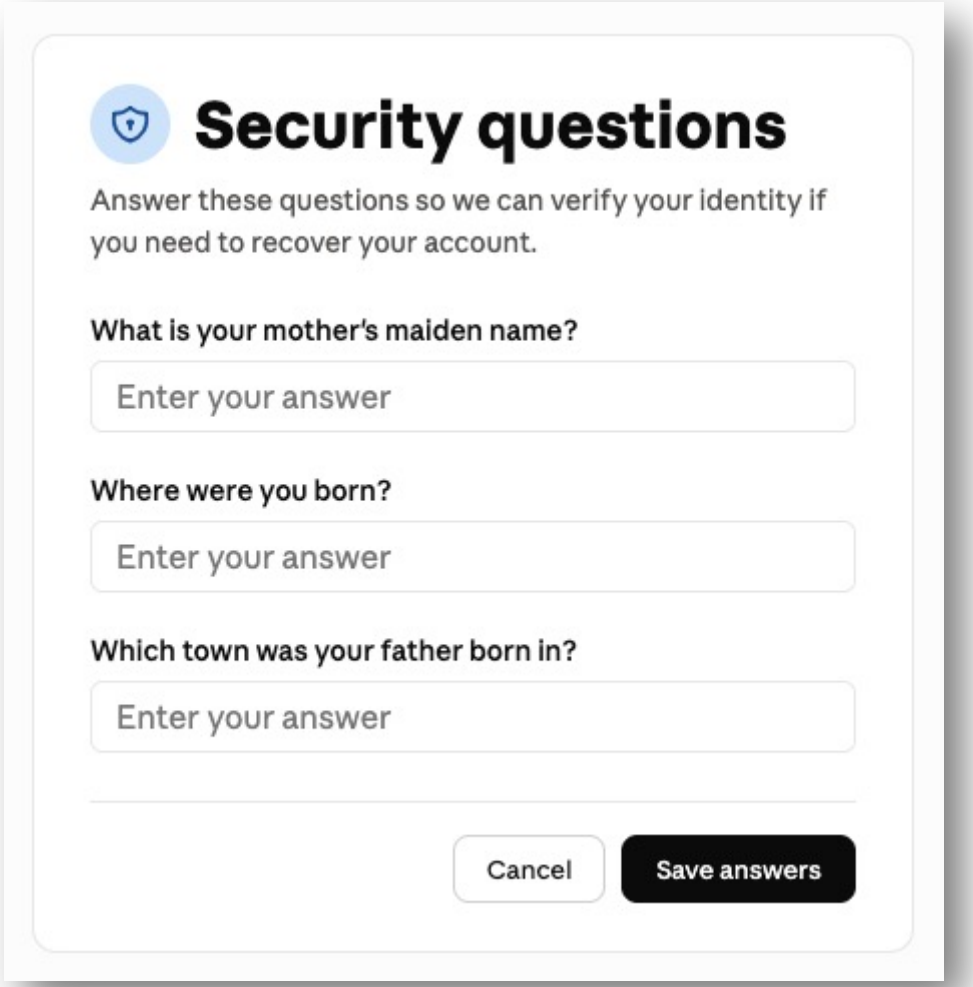
Sarah Vieweg
Qatar Computing Research Institute
Doha, Qatar
svieweg@qf.org.qa

the wrong privacy setting. Even though I always had my privacy setting on pretty high. The only things I allow to be shown are the things I allow. I have ten different friends groups. I have 'limited', 'more limited' 'most limited'...I have six to seven different levels of privacy."

Assumed cultural context (Contextus praesumptus)



Assumed cultural context (Contextus praesumptus)



“Not my problem” (Res nullius)

Natural habitat: any large organization
M.O.M. Classification: XXXXX
LINDDUN: non-compliance, data disclosure, sooner or later the other 5
Notable (dark) magical uses: shipping fast and breaking things
Data diet: EVERYTHING



“Not my problem” (Res nullius)

Engineering Privacy by Design: Are engineers ready to live up to the challenge?

Kathrin Bednar[a], Sarah Spiekermann[a], and Marc Langheinrich[b]

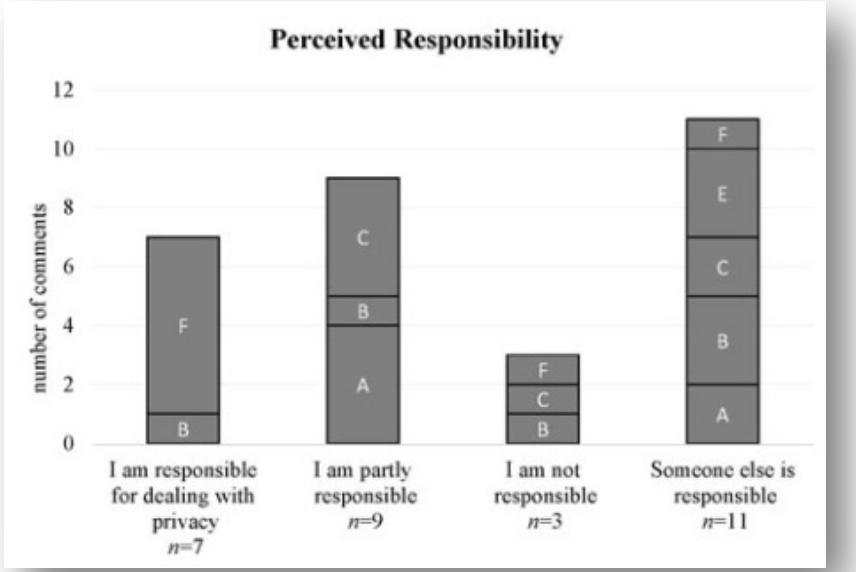
[a]Institute for Information Systems and Society, Vienna University of Economics and Business, Vienna, Austria; [b]Faculty of Informatics, Università della Svizzera Italiana, Lugano, Switzerland

“Not my problem” (Res nullius)

Engineering Privacy by Design: Are engineers ready to live up to the challenge?

Kathrin Bednar[a], Sarah Spiekermann[a], and Marc Langheinrich[b]

[a]Institute for Information Systems and Society, Vienna University of Economics and Business, Vienna, Austria; [b]Faculty of Informatics, Università della Svizzera Italiana, Lugano, Switzerland

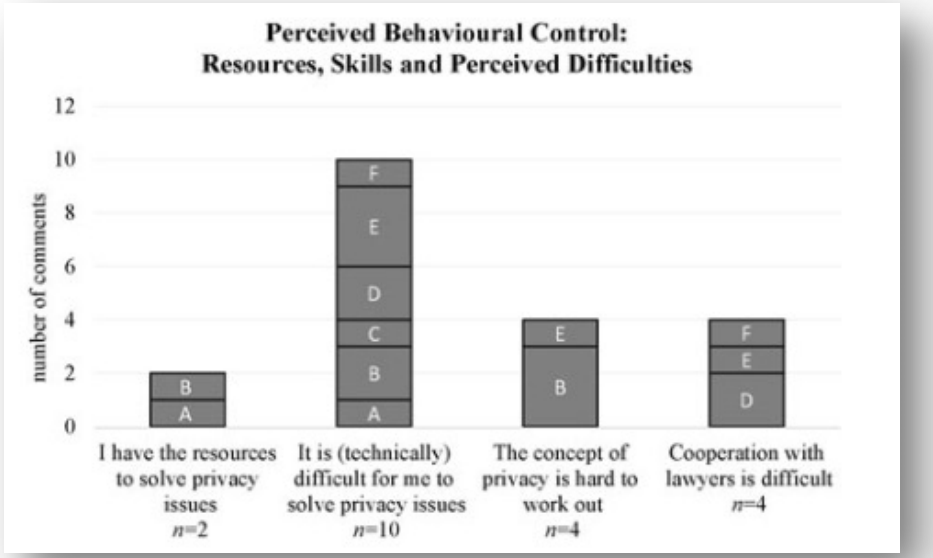


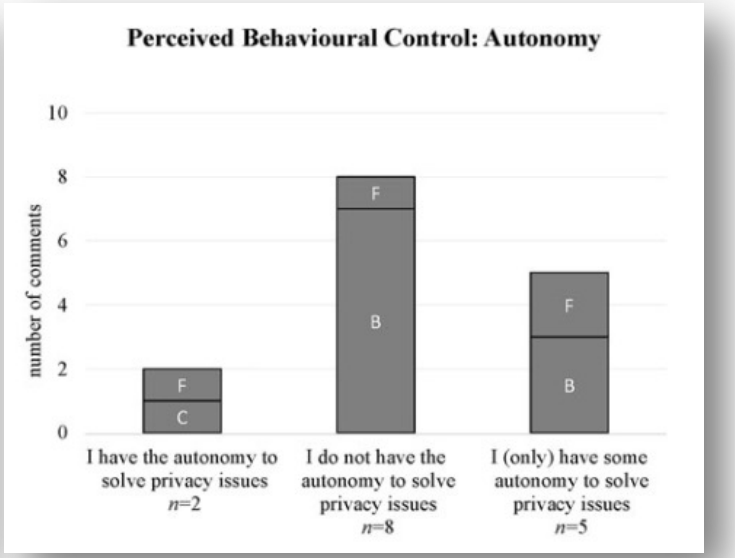
“Not my problem” (Res nullius)

Engineering Privacy by Design: Are engineers ready to live up to the challenge?

Kathrin Bednar[a], Sarah Spiekermann[a], and Marc Langheinrich[b]

[a]Institute for Information Systems and Society, Vienna University of Economics and Business, Vienna, Austria; [b]Faculty of Informatics, Università della Svizzera Italiana, Lugano, Switzerland





“Not my problem” (Res nullius)

Company-wide comms: “As part of our ✨ AI transformation ✨, we expect all employees to adopt OpenAI Codex and work in GitHub.”

Account Manager wonders: “So can we store customer account data in GitHub repos now? Before we were told to only use Excel.”

“Not my problem” (Res nullius)

How might this play out in your organization? Who would the Account Manager ask the question to? Would the question ever reach your team?

“Not my problem” (Res nullius)

Can we store customer account data in GitHub?

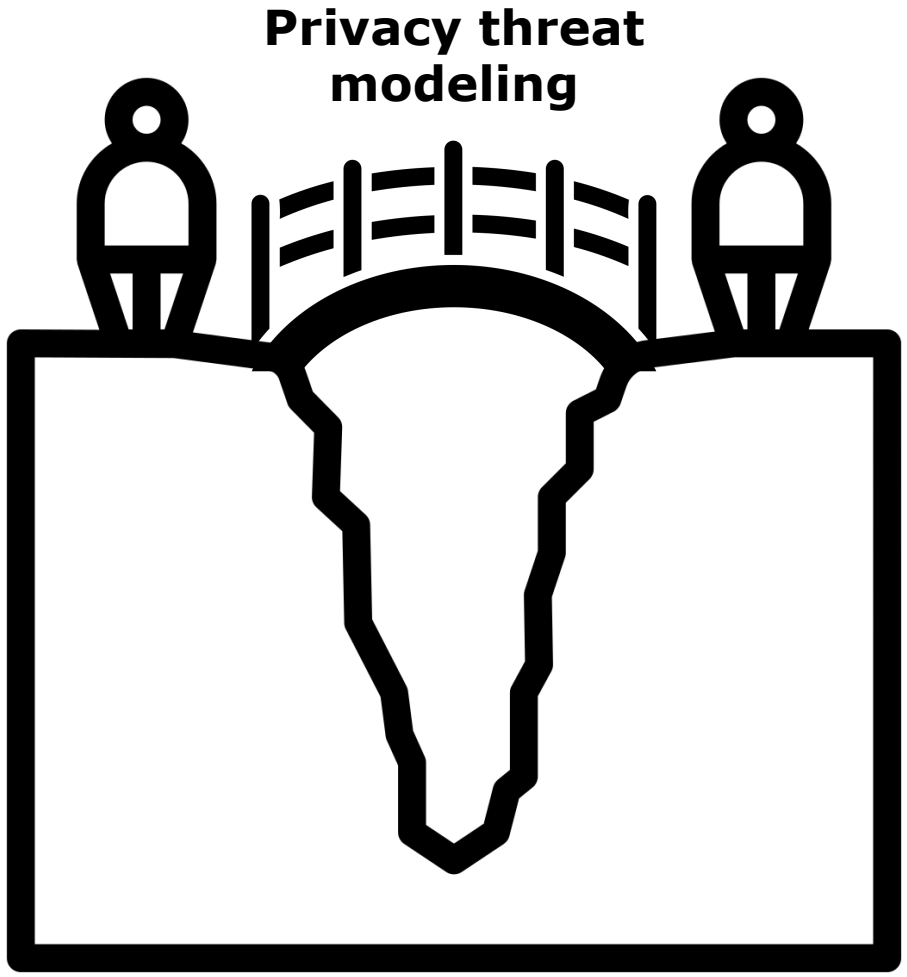
Privacy Legal team	(hon. mention) Privacy Operations	Technical team (IT / Security / SRE / PrivEng)
• May not be expected or even *allowed* to assess risk beyond bare minimum for legal and contractual compliance • Checks cross-border data transfer and contractual safeguards • DPIA threshold not met • Assessment: **low risk**		• Expected to assess and mitigate technical risk • Handled recent incidents of employees new to GitHub making repos public by accident • Assessment: **high risk** until GitHub Enterprise controls are fully implemented

“Not my problem” (Res nullius)

We need to break down these org silos to effectively privacy threat model.
The good news: getting started with threat modeling is one way to address silos!



“Not my problem” (Res nullius)



Your turn! What was the last privacy threat you tackled?

Natural habitat: ??
M.O.M. Classification: ??
LINDDUN threat(s): ??
Notable (dark) magical uses: ??
Data diet: ??
Handling instructions: ??



Q&A