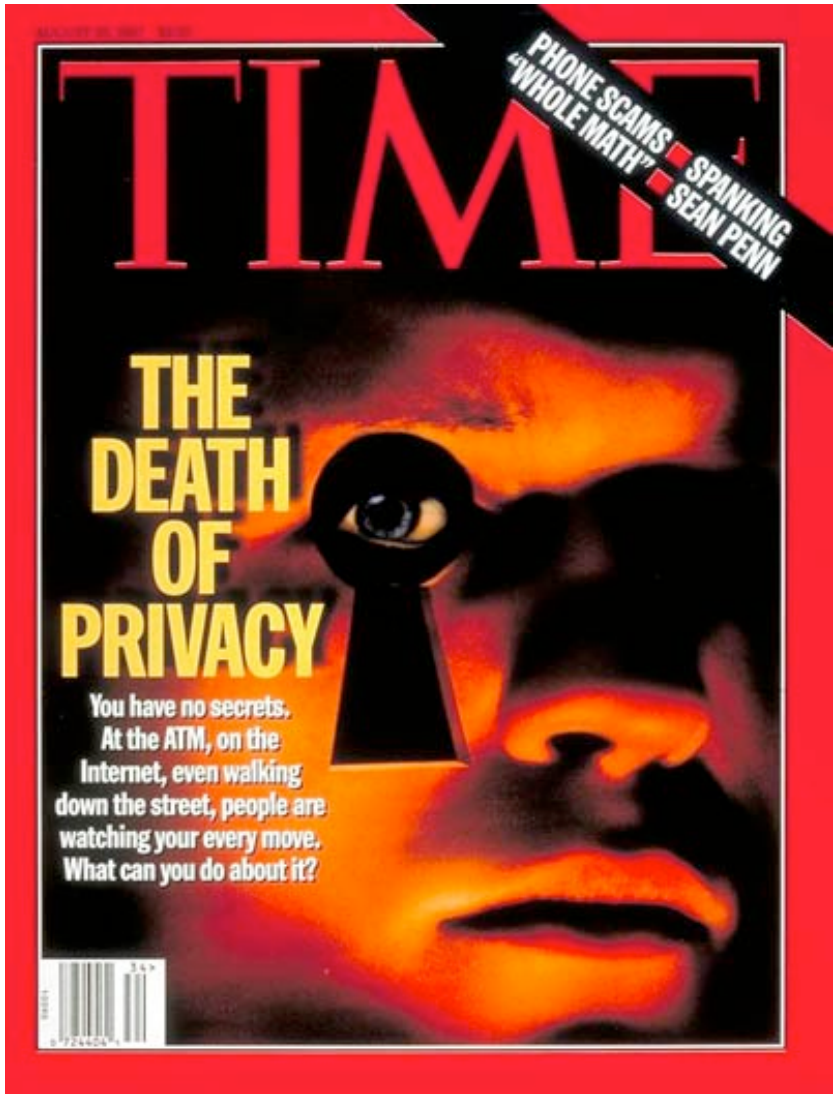
Paradigms of Privacy Research & Privacy Engineering

Seda Gürses
f.s.gurses@tudelft.nl
TU Delft/ KU Leuven

18. June 2019


TIME
PHONE SCAMS
"WHOLE MATH"
SPANKING
SEAN PENN
THE DEATH OF PRIVACY
You have no secrets. At the ATM, on the Internet, even walking down the street, people are watching your every move. What can you do about it?


Gauging the allure of designer drugs p. 469
Blown-up brains for a better inside view pp. 474 & 543
Single-crystal perovskite solar cells pp. 519 & 522
Science
$10
30 JANUARY 2015
sciencemag.org
AAAS
SPECIAL ISSUE
The End of
PRIVACY


PET SEMATARY
©2009 Last Legion Games, LLC. All Rights Reserved.

GDPR requires data protection by design and by default (Article 25)

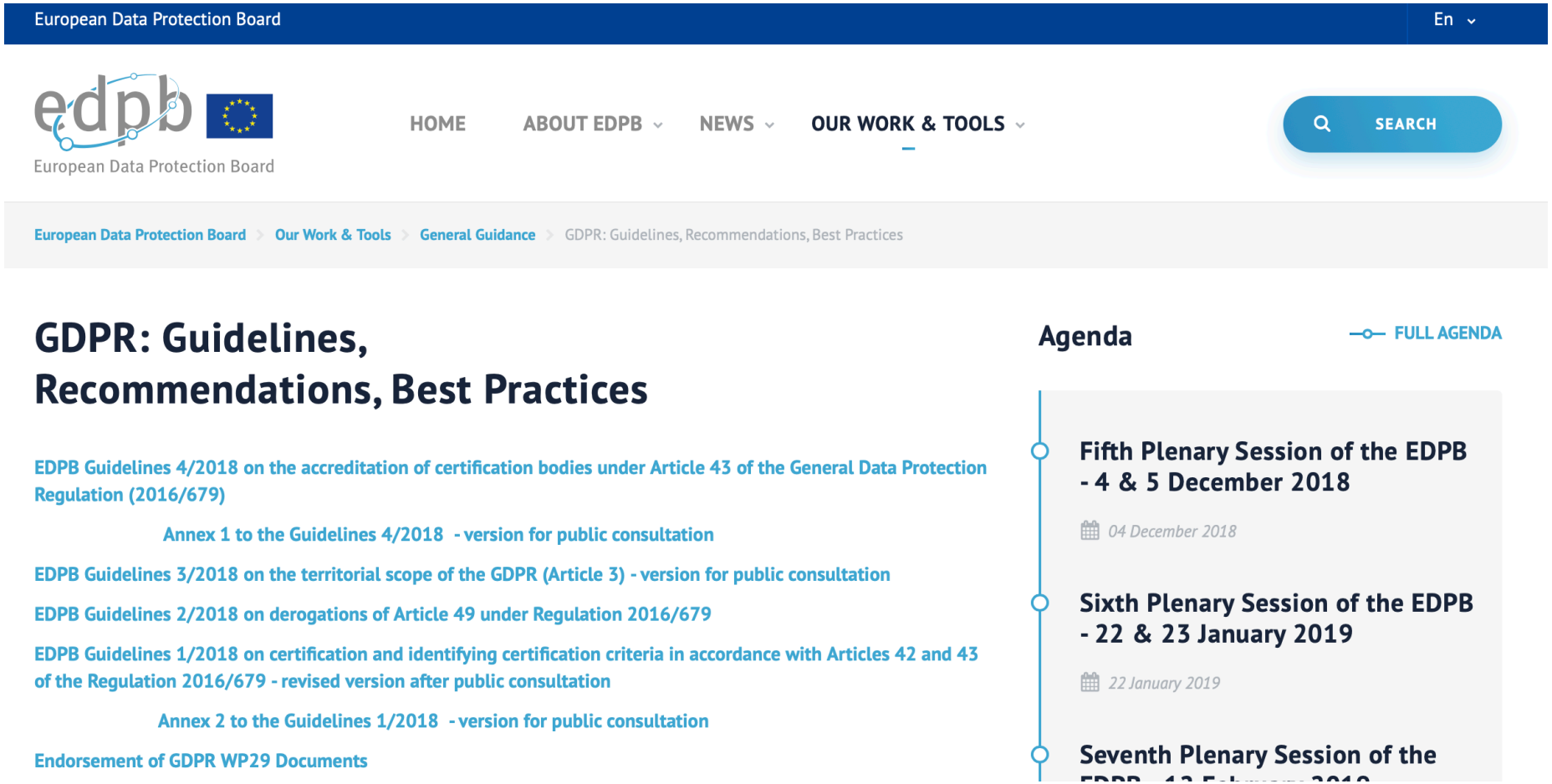
A complex law with many requirements.

More about creating a vision than a checklist

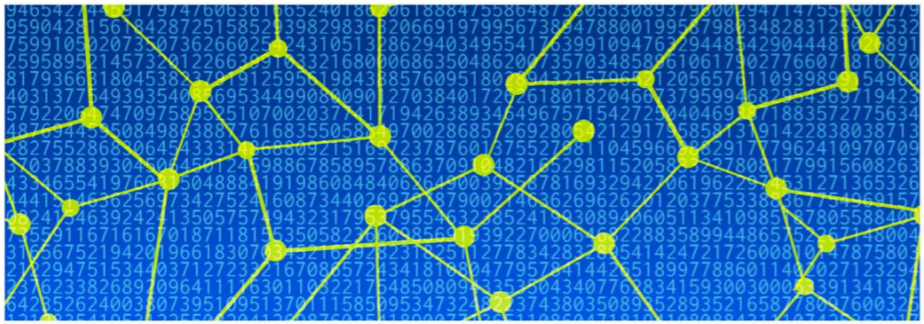
How to of Article 25!?

recommendations are abundant

European Data Protection Board
https://edpb.europa.eu/edpb_en



European Data Protection Supervisor
https://edps.europa.eu



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2018

Preliminary Opinion on privacy by design

ENISA
https://www.enisa.europa.eu/publications

Privacy and Data Protection by Design

This report contributes to bridging the gap between the legal framework and the available technolog-ical implementation measures by providing an inventory of existing approaches, privacy design strat-egies, and technical building blocks of various degrees of maturity from research and development. Starting from the privacy principles of the legislation, important elements are presented as a first step towards a design process for privacy-friendly systems and services.

Published January 12, 2015
Language English

Privacy by design in big data

The extensive collection and further processing of personal information in the context of big data analytics has given rise to serious privacy concerns, especially relating to wide scale electronic surveillance, profiling, and disclosure of private data. In order to allow for all the benefits of analytics without invading individuals' private sphere, it is of utmost importance to draw the limits of big data processing and integrate the appropriate data protection safeguards in the core of the analytics value chain. ENISA, with the current report, aims at supporting this approach, taking the position that, with respect to the underlying legal obligations, the challenges of technology (for big data) should be addressed by the opportunities of technology (for privacy).

Published December 17, 2015
Language English

Norwegian Data Protection Authority
https://www.datatilsynet.no

Datatilsynet

Guide

Software development with Data Protection by Design and by Default

The Norwegian Data Protection Authority has developed these guidelines to help organisations understand and comply with the requirement of data protection by design and by default in article 25 of the General Data Protection Regulation. We have cooperated with security professionals and software developers in public and private sector among others.

Print guide

Unabhängiges Landeszentrum für Datenschutz
https://www.datenschutzzentrum.de/sdm/

Federal Trade Commission
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/tech

Mobile Health App Developers: FTC Best Practices

TAGS: Advertising and Marketing | Health Claims | Privacy and Security | Consumer Privacy | Data Security | Tech | Health Care

When developing a health app, sound privacy and security practices are key to consumer confidence. Here are some best practices to help you build privacy and security into your app. These practices also can help you comply with the FTC Act.

Start with Security: A Guide for Business offers tips for any business wanting to implement sound data security. For health app developers, here's tailored advice and additional questions to ask.

- Minimize data.
- Limit access and permissions.
- Keep authentication in mind.
- Consider the mobile ecosystem.
- Implement security by design.
- Don't reinvent the wheel.
- Innovate how you communicate with users.
- Don't forget about other applicable laws.

National Institute of Standards and Technology (NIST)
https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering

PRIVACY ENGINEERING PROGRAM

About +
Collaboration Space +
Resources
Events
Get Involved

Resources

NIST Internal Report (NISTIR) 8062: *An Introduction to Privacy Engineering and Risk Management in Federal Systems*

NISTIR 8062 introduces the concept of applying systems engineering practices to privacy and provides a new model for conducting privacy risk assessments on federal systems.

PDF

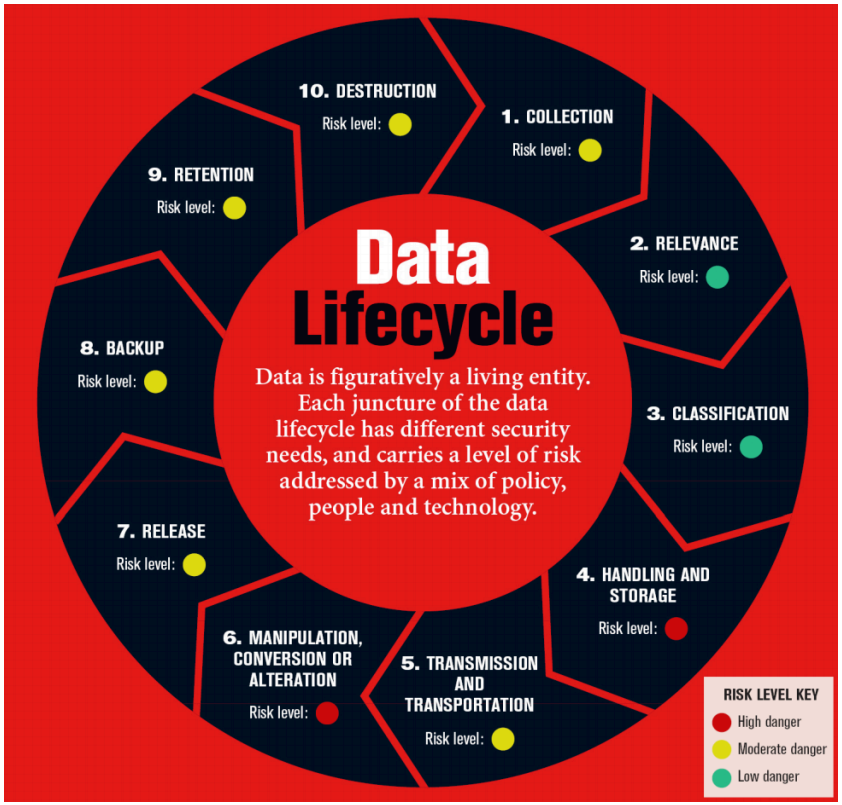
More content coming soon!

Data Protection as a Service

Accountability Life Cycle Activities

The table below lists the phased activities that support the Accountability Life Cycle.

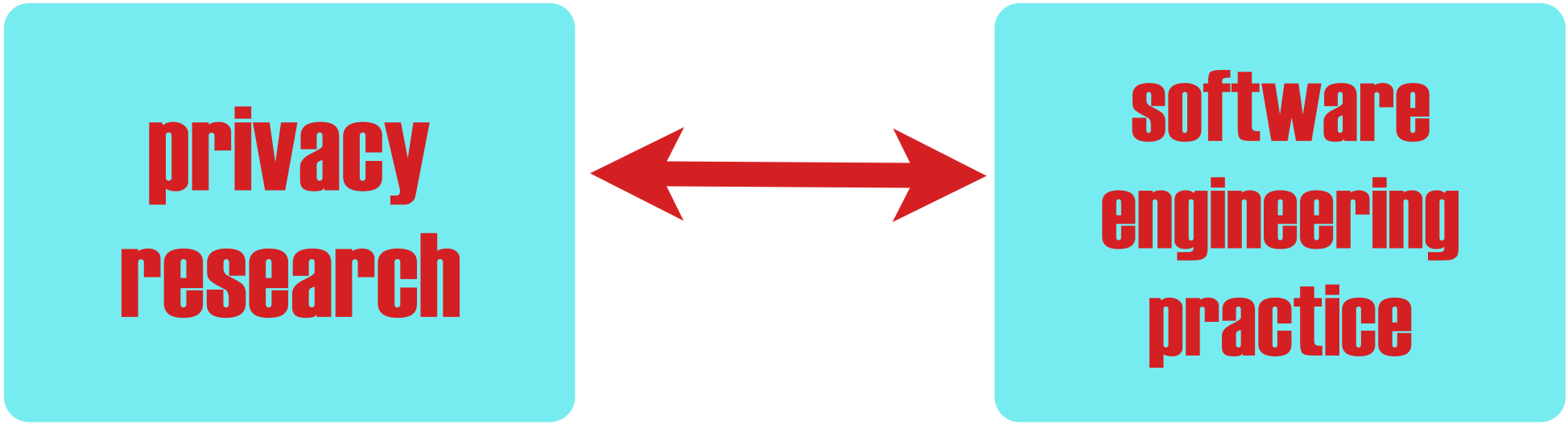
Phase	Activity
PHASE I: Prepare	Activity A: Obtain the buy-in of key business stakeholders Activity B: Establish your GDPR readiness program team Activity C: Identify and assess relevant business functions Activity D: Identify and assess in-scope Third Party Processing activities Activity E: Establish a central Personal Data register Activity F: Distribute updated Data Protection policies and Privacy Notices Activity G: Educate internal Personal Data Handlers and external Data Processors
PHASE II: Operate	Activity H: Disseminate and maintain external Privacy Notices Activity I: Justify and record lawful Processing mechanisms Activity J: Process and record Data Subject rights requests Activity K: Validate and record Third Country data transfers Activity L: Report and manage Personal Data Breach incidents
PHASE III: Maintain	Activity M: Evidence understanding of Data Protection policies Activity N: Ensure the ongoing integrity and quality of the Personal Data Processing register Activity O: Trigger impact assessments for business change events Activity P: Verify compliance of Third Party Personal Data Processing activities Activity Q: Demonstrate effectiveness of Personal Data handling practices

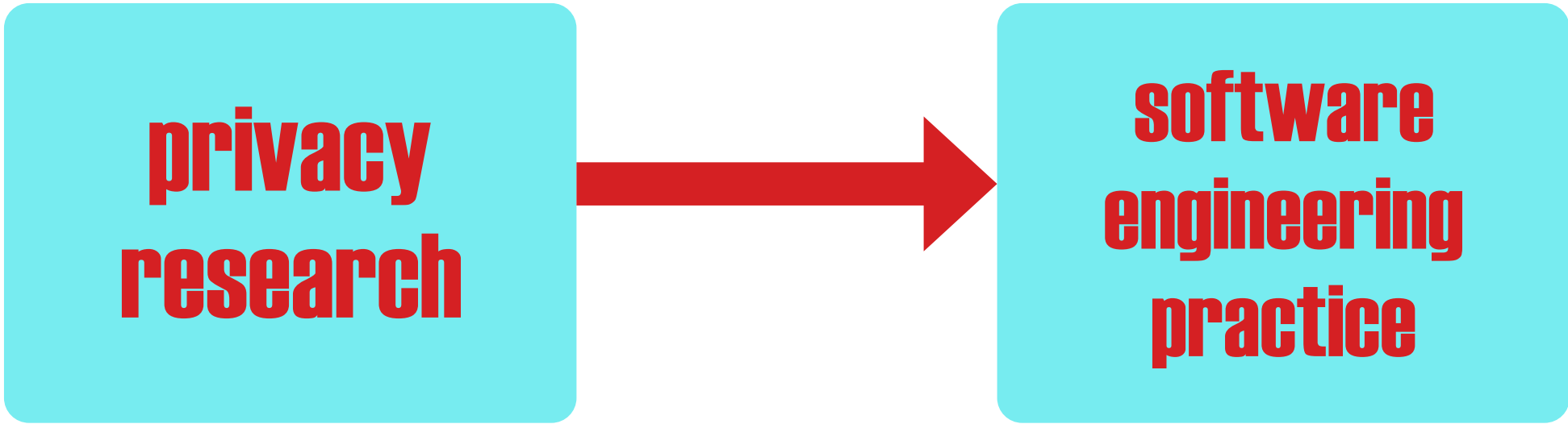


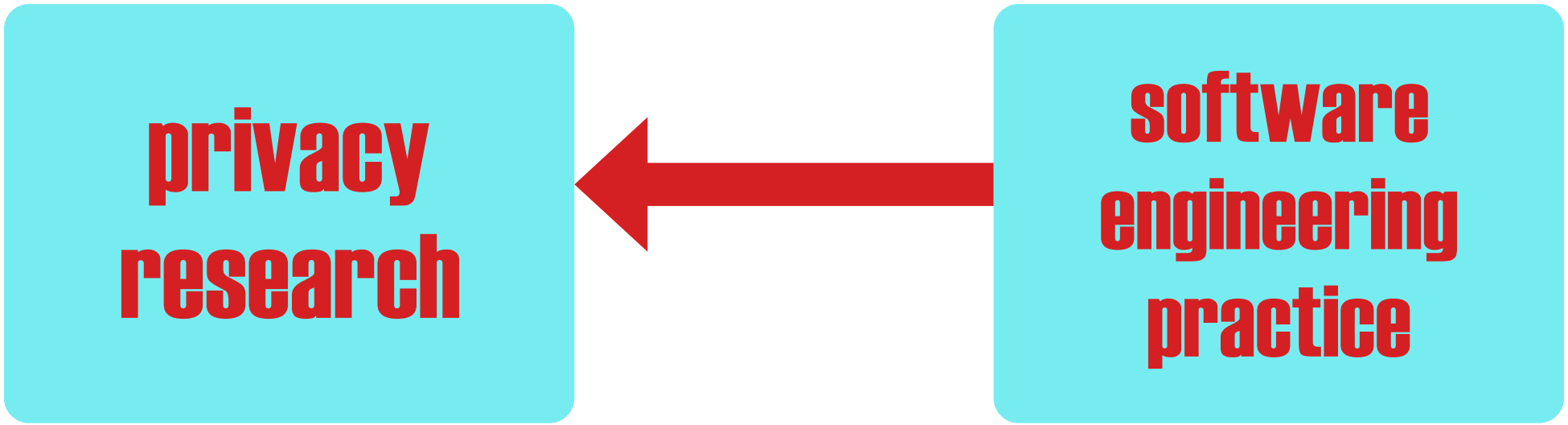
http://cdn.ttgtmedia.com/informationsecurity/images/vol4iss7/ism_v4i7_f4_DataLifecycle.pdf

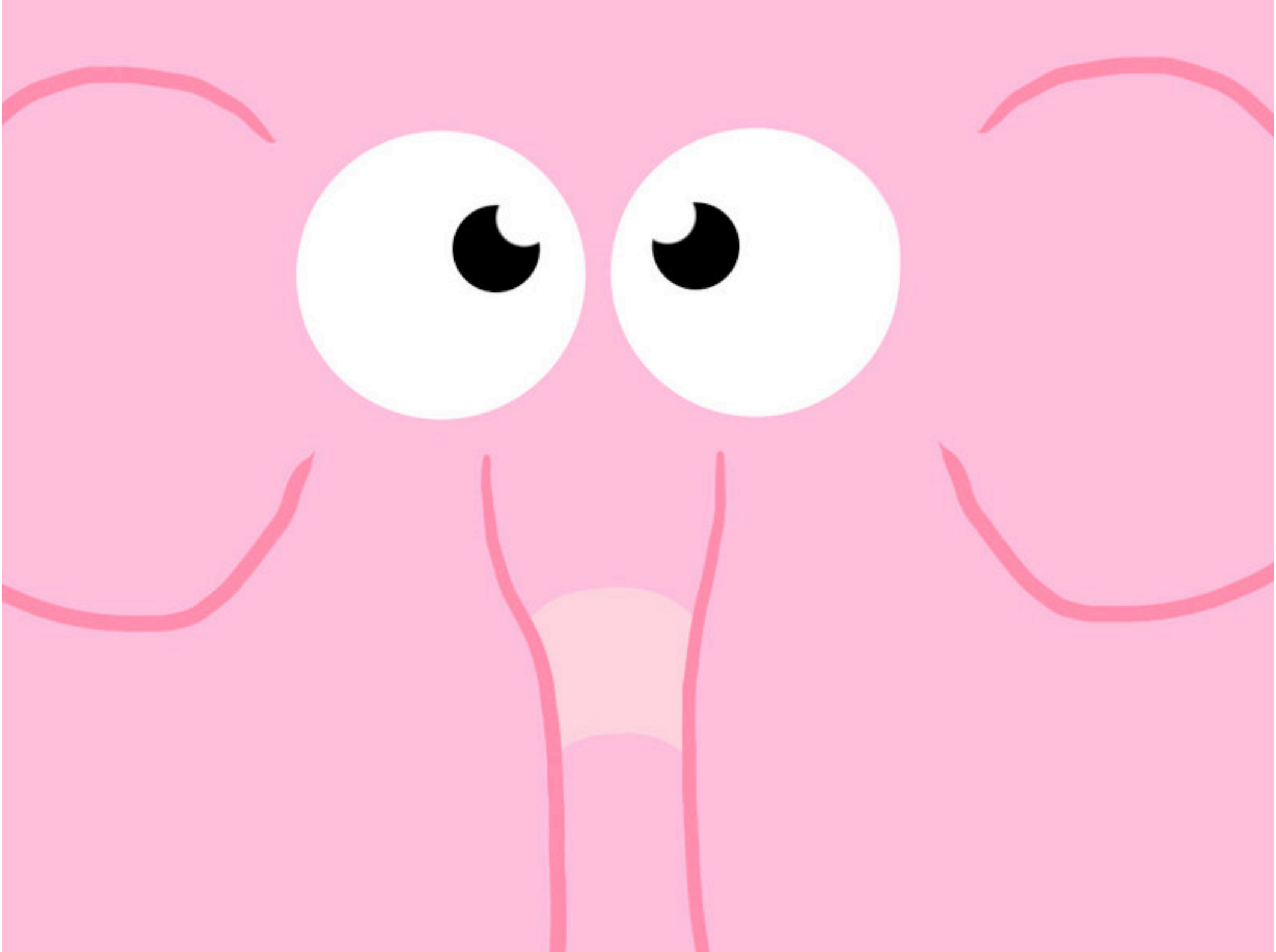
getting privacy engineering right?

getting privacy engineering right?

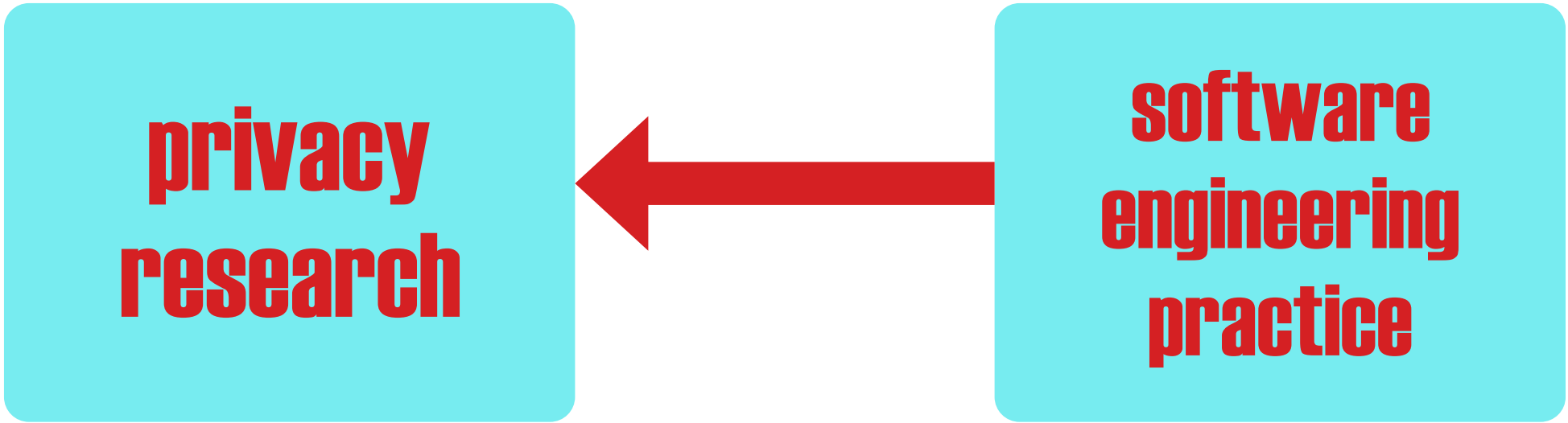



privacy research
software engineering practice


privacy research
software engineering practice

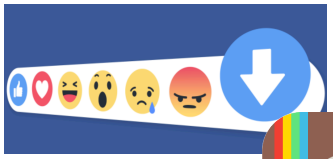


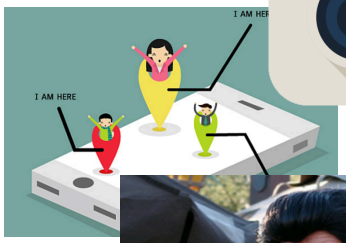
can it be that the practices around the production of software are an important element of privacy research?



matters?

800





1.6b
SWIPES PER DAY

26m
MATCHES PER DAY

20b+
TOTAL MATCHES

190+
COUNTRIES

1.5m
DATES PER WEEK

TINDER PRIVACY POLICY

Last Updated: 10/26/2017

We take security measures to help safeguard your personal information from unauthorized access and disclosure. However, no system can be completely secure. Therefore, although we take steps to secure your information, we do not promise, and you should not expect, that your personal information, chats, or other communications will always remain secure. Users should also take care with how they handle and disclose their personal information and should avoid sending personal information through insecure email. Please refer to the

gcwelborn/tinder-scraper

A Tinder Bot for Data Scientist's ⚒ 🔥

http://cruzwelborn.com/tinder-scraper/

Someone scraped 40,000 Tinder selfies to make a facial dataset for AI experiments

Posted Apr 28, 2017 by Natasha Lomas (@riptari)

It might be a pseudo science, but students take the threat of eugenics seriously

Today's white nationalists and neo-Nazis make extensiv use of racist pseudo-science to bolster their political arguments.

Profiling and ranking is becoming a common practice

Tinder decides based on your profile who you see first!

LinkedIn uses similar inferences to decide which job ads to show you!

Insurance companies, banks, universities, and many others are ready to follow suit!

scenario

imagine you want to share a picture on a social network.

picture of a meeting with your colleagues discussing the introduction of code commits as a performance metric

you want to share the excitement of the moment with your friends (not your manager)

How would you use OR design a system to do the following?

you would like to tag your colleagues in the picture in an appropriate manner

you do not want your managers and 3rd parties (like Tinder) to see the picture

you do not want the social network to run facial recognition on the pictures

study:
lit review
42 interviews
events/papers

PRIVACY RESEARCH PARADIGMS

privacy as confidentiality

privacy as control

privacy as practice

PRIVACY RESEARCH PARADIGMS

privacy as confidentiality

- "the right to be let alone" Warren and Brandeis
- data minimization
- properties with mathematical guarantees
- avoid single point of failure
- open source - it takes a village to keep it secure

PRIVACY RESEARCH PARADIGMS

privacy as confidentiality

you are worried that the social network may run facial recognition

encrypt the picture before uploading

obfuscate the image

PRIVACY RESEARCH PARADIGMS

privacy as confidentiality

secure messaging

- Signal – WhisperSystems
- WhatsApp – Facebook
- iMessage – Apple
- Off The Record – Cypherpunks

All Tools	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Off-The-Record Messaging for Mac (Adium)							
Off-The-Record Messaging for Windows (Pidgin)							
PGP for Mac (GPGTools)							
PGP for Windows Gpg4win							

TABLE II

CONVERSATION SECURITY PROTOCOLS AND THEIR USABILITY AND ADOPTION IMPLICATIONS. NO APPROACH REQUIRES ADDITIONAL USER EFFORT.

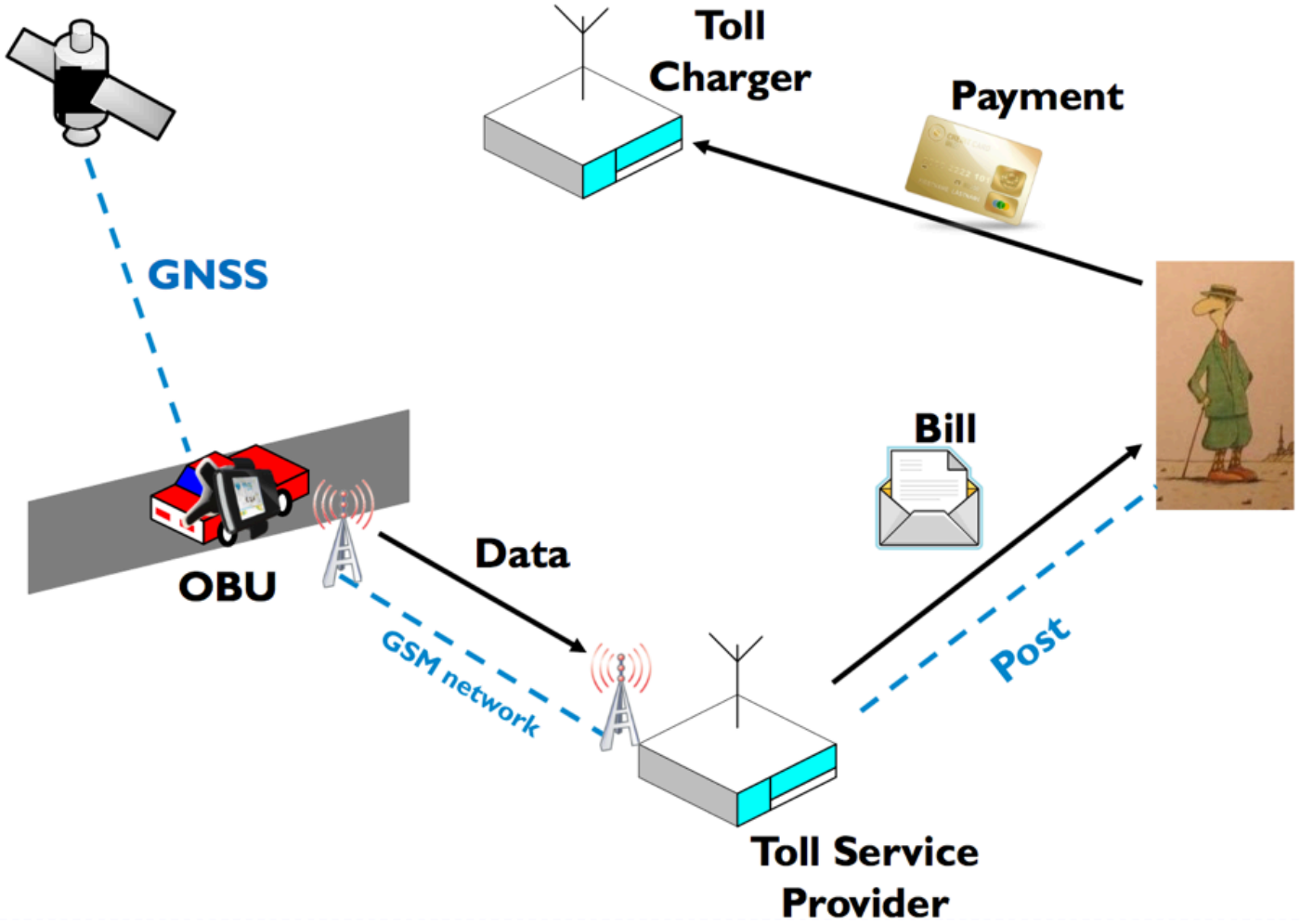
Scheme	Example	Security and Privacy													Adoption					Group Chat				
		Confidentiality	Integrity	Authentication	Participant Consistency	Destination Validation	Forward Secrecy	Backward Secrecy	Anonymity Preserving	Speaker Consistency	Causality Preserving	Global Transcript	Message Unlinkability	Message Repudiation	Particip. Repudiation	Out-of-Order Resilient	Dropped Message Resilient	Asynchronicity	Multi-Device Support	No Additional Service	Computational Equality	Trust Equality	Subgroup Messaging	Contractable	Expandable
TLS+Trusted Server†*	Skype	-	-	-	-	-	-	-	-	-	-	●	●	●	●	●	●	●	-	●	●	●	◐	◐
Static Asymmetric Crypto†*	OpenPGP, S/MIME	●	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	●	●	●				
+IBE†	Wang et al.	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	●	●	-				
+Short Lifetime Keys	OpenPGP Draft	●	●	●	-	-	◐	◐	●	-	-	-	-	-	-	●	●	●	●	-				
+Non-Interactive IBE†	Canetti et al.	●	●	●	-	-	●	-	●	-	-	-	-	-	-	◐	●	●	●	●				
+Puncturable Encryption†	Green and Miers	●	●	●	-	-	●	-	●	-	-	-	-	-	-	●	●	●	●	●				
Key Directory+Short Lifetime Keys†	IMKE	●	●	◐	-	●	◐	◐	-	-	-	-	●	●	●	●	●	-	-	-				
+Long-Term Keys†	SIMPP	●	●	◐	-	●	◐	◐	-	-	-	-	●	●	-	●	●	-	-	-				
Authenticated DH†*	TLS-EDH-MA	●	●	●	●	●	◐	◐	●	-	-	-	●	●	◐	●	●	-	-	●				
+Naïve KDF Ratchet*	SCIMP	●	●	●	●	●	●	◐	●	◐	-	-	●	●	◐	◐	◐	-	-	●				
+DH Ratchet†*	OTR	●	●	●	●	●	◐	●	●	◐	◐	-	●	●	◐	◐	◐	-	-	●				
+Double Ratchet†*	Axolotl	●	●	●	●	●	●	●	●	◐	◐	-	●	●	◐	●	◐	-	-	●				
+Double Ratchet+3DH AKE†*	-	●	●	●	●	●	●	●	◐	◐	◐	-	●	●	●	●	◐	-	-	●				
+Double Ratchet+3DH AKE+Prekeys†*	TextSecure	●	●	●	●	●	●	●	-	◐	●	-	●	●	●	◐	◐	●	-	-				
Key Directory+Static DH+Key Transport†	Kikuchi et al.	●	●	-	-	●	◐	◐	-	-	-	-	●	●	-	●	●	●	-	-	-	-	-	●	●
+Authenticated EDH+Group MAC†	GROK	●	●	◐	-	●	◐	◐	●	-	-	-	●	●	-	●	●	●	-	-	-	-	-	●	●
GKA+Signed Messages+Parent IDs†	OldBlue	●	●	●	●	●	◐	◐	●	●	●	-	-	-	-	●	●	◐	-	●	●	●	-	-	-
Authenticated MP DH+Causal Blocks†*	KleeQ	●	●	◐	◐	◐	●	●	●	◐	◐	●	-	●	●	●	●	◐	-	●	●	●	-	-	●
OTR Network+Star Topology†	GOTR (2007)	●	●	-	-	-	◐	●	-	-	-	-	●	●	●	◐	●	◐	-	●	-	-	-	●	●
+Pairwise Topology†		●	●	●	●	●	◐	●	●	-	-	-	●	●	●	◐	●	◐	-	●	●	●	●	●	●
+Pairwise Axolotl+Multicast Encryption*	TextSecure	●	●	●	-	●	●	●	-	●	●	-	●	●	●	●	●	●	-	-	●	●	●	●	●
DGKE+Shutdown Consistency Check†	mpOTR	●	●	●	●	●	◐	◐	●	◐	-	-	-	●	●	●	●	-	-	●	●	●	-	-	-
Circle Keys+Message Consistency Check†	GOTR (2013)	●	●	●	●	●	◐	◐	●	●	●	●	●	●	●	●	-	-	-	◐	●	●	-	●	●

● = provides property; ◐ = partially provides property; - = does not provide property; †has academic publication; *end-user tool available

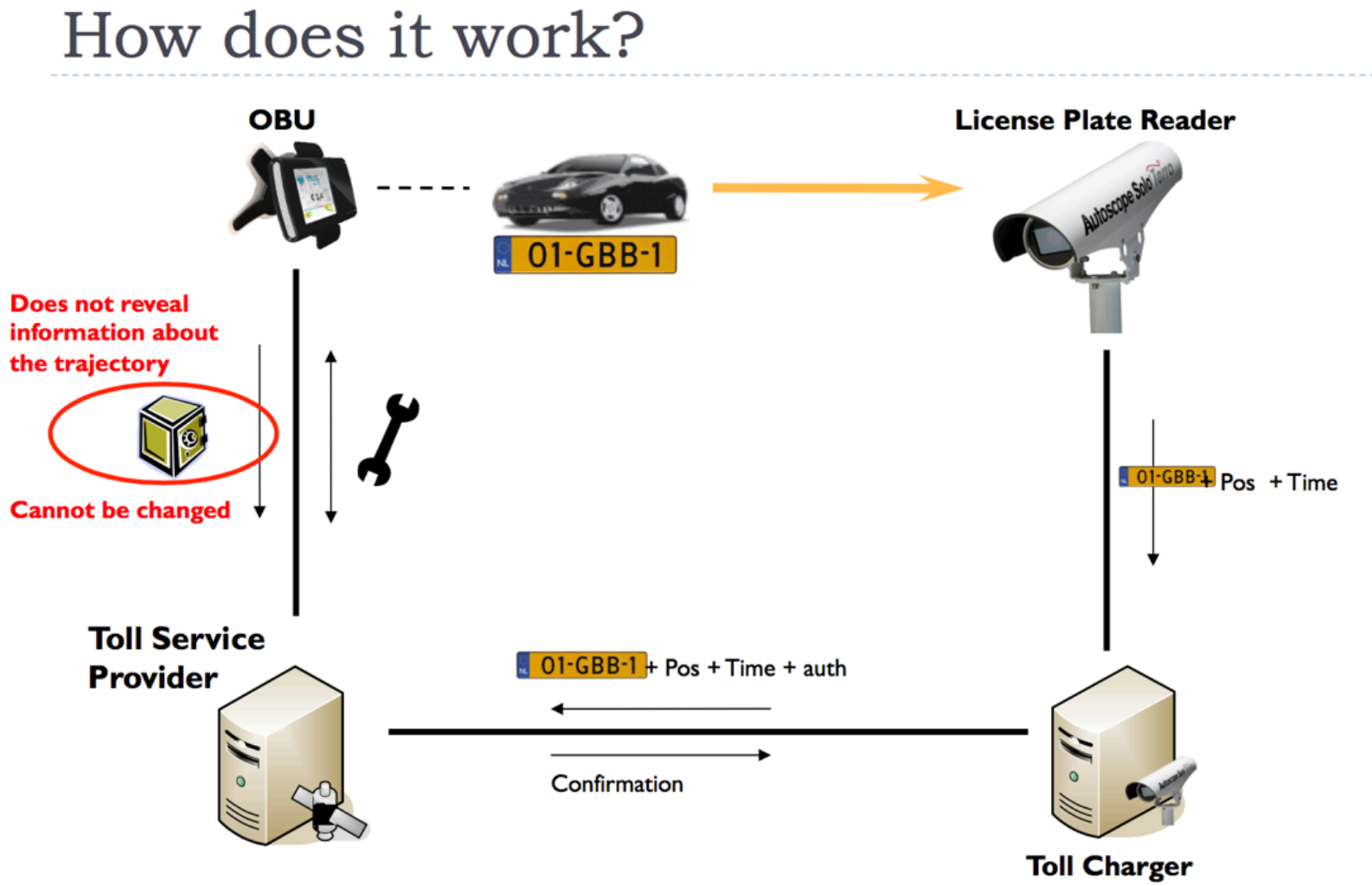
Security and Privacy												Adoption					Group Chat			
Confidentiality	Integrity	Authentication	Participant Consistency	Destination Validation	Forward Secrecy	Backward Secrecy	Anonymity Preserving	Speaker Consistency	Causality Preserving	Global Transcript	Message Unlinkability	Message Repudiation	Particip. Repudiation	Out-of-Order Resilient	Dropped Message Resilient	Asynchronicity	Multi-Device Support	No Additional Service	Computational Equality	Trust Equality	Subgroup Messaging	Contractable	Expandable

data minimization

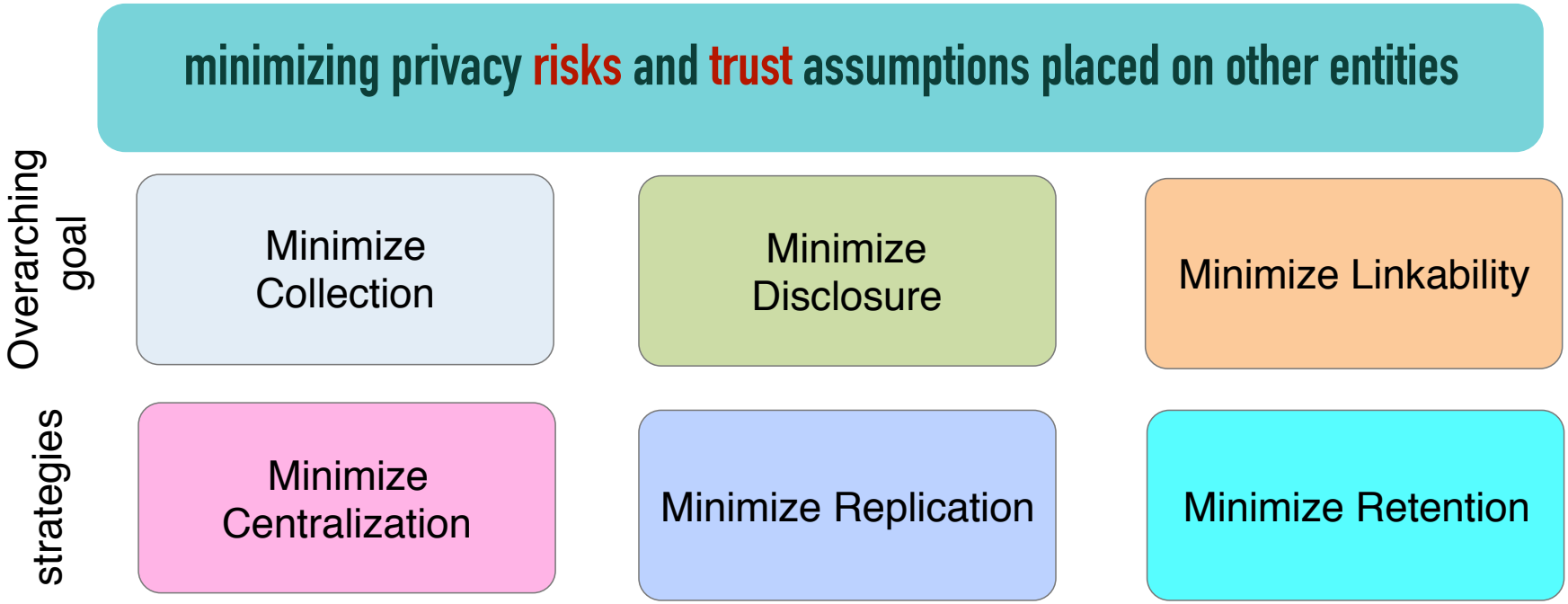
EETS straightforward implementation



data minimization



Unpacking Data Minimization: Privacy By Design Strategies



Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design Reloaded. Amsterdam Privacy Conference. 2015

PRIVACY RESEARCH PARADIGMS

privacy as control

"right of the individual to decide what information about himself should be communicated to others and under what circumstances" Westin

transparency and accountability

FIPPS/GDPR compliance

individual participation and control

control sharing of picture with managers and 3rd parties

FB and CambridgeAnalytica

PRIVACY RESEARCH PARADIGMS

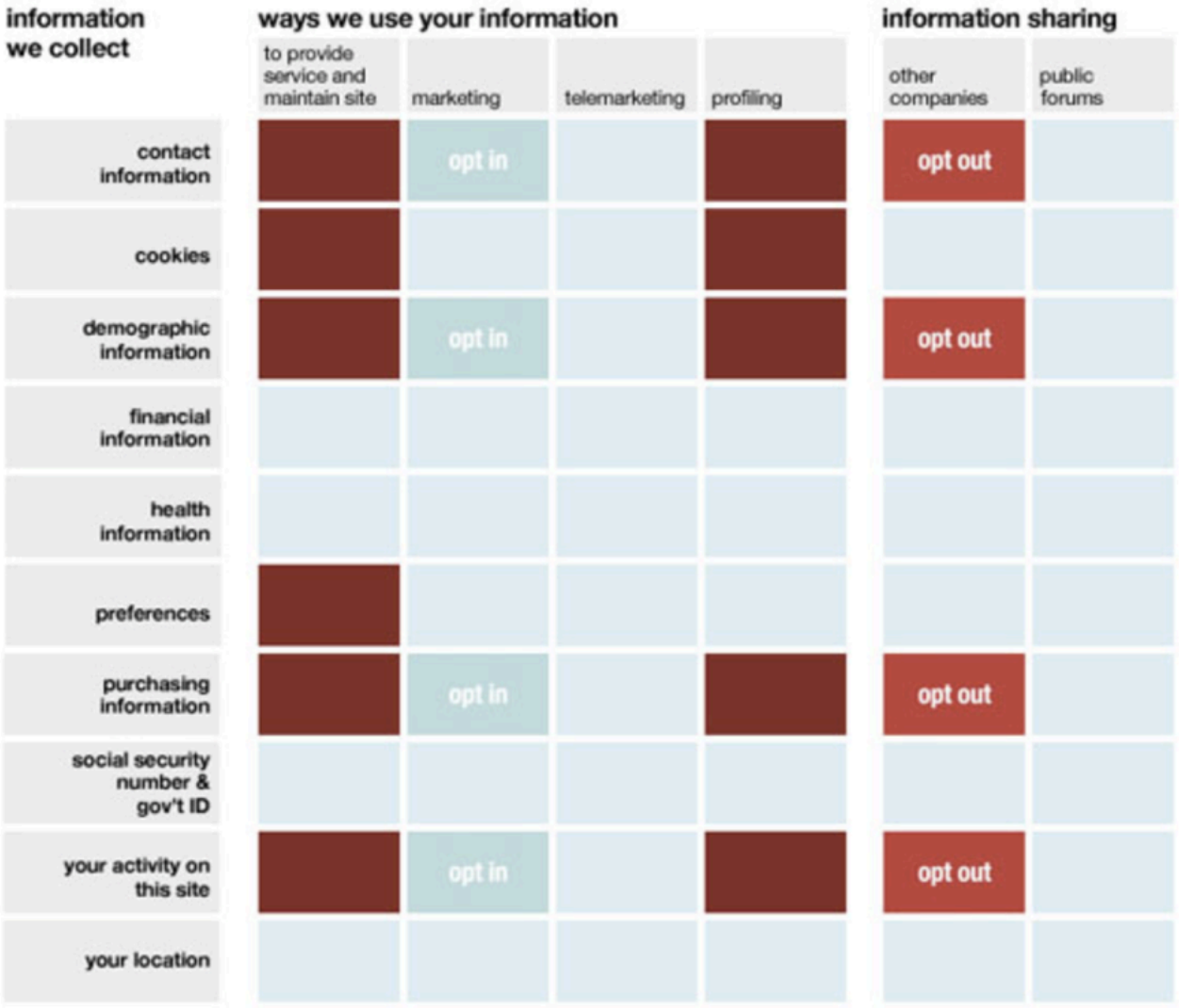
privacy as control

privacy policy languages

purpose based access control

Attribute Based Credentials

Bell Group



Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

bell.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@bell.com

Eddy

a privacy specification language

Return to Main Page

Eddy is a privacy requirements specification language that privacy analysts can use to express requirements over acts to collect, use, transfer and retain personal and technical information. The language uses a simple SQL-like syntax to express whether an action is permitted or prohibited, and to restrict those statements to particular data subjects and purposes. The Eddy specifications are compiled into Description Logic to automatically detect conflicting requirements and to trace data flows within and across specifications. Each specification can describe an organization's data practices, or the data practices of specific components in a software architecure.

For further technical details on Eddy, please see our relevant publications:

1. **Detecting Repurposing and Over-collection in Multi-party Privacy Requirements Specifications**
   Travis D. Breaux, Daniel Smullen, Hanan Hibshi. To Appear: *23rd IEEE International Requirements Engineering Conference*, Ottawa, Canada, 2015. (pdf)

2. **Eddy, A Formal Language for Specifying and Analyzing Data Flow Specifications for Conflicting Privacy Requirements**
   Travis D. Breaux, Hanan Hibshi, Ashwini Rao. *Requirements Engineering Journal,* 19(3): 281-307, 2014. (doi). This an extended journal version of our conference paper (doi) that was nominated for best paper and presented at IEEE RE'13 (slides)

We provide interactive examples below to demonstrate the Eddy language, and the Java source code is available on GitHub (source) under GPLv2.

View and analyze an existing example
Example specification to illustrate conflict analysis
Example specification to illustrate flow analysis
Example specification to illustrate use limitation analysis

Android Permissions Remystified: A field study of Contextual Integrity (Wijesekera et al. 2015)

When to actually prompt

Privacy violations occur when ***sensitive information*** is used in ways ***defying users' expectations***.

Helen Nissenbaum, *Privacy as Contextual Integrity*. Washington Law Review 79, 2004.

Android Permissions Remystified: A field study of Contextual Integrity (Wijesekera et al.)

The experiment

36 Android smartphone users

6,048 hours of real-world use

27 million permission requests

Android Permissions Remystified: A field study of Contextual Integrity (Wijesekera et al.)

Users want a choice

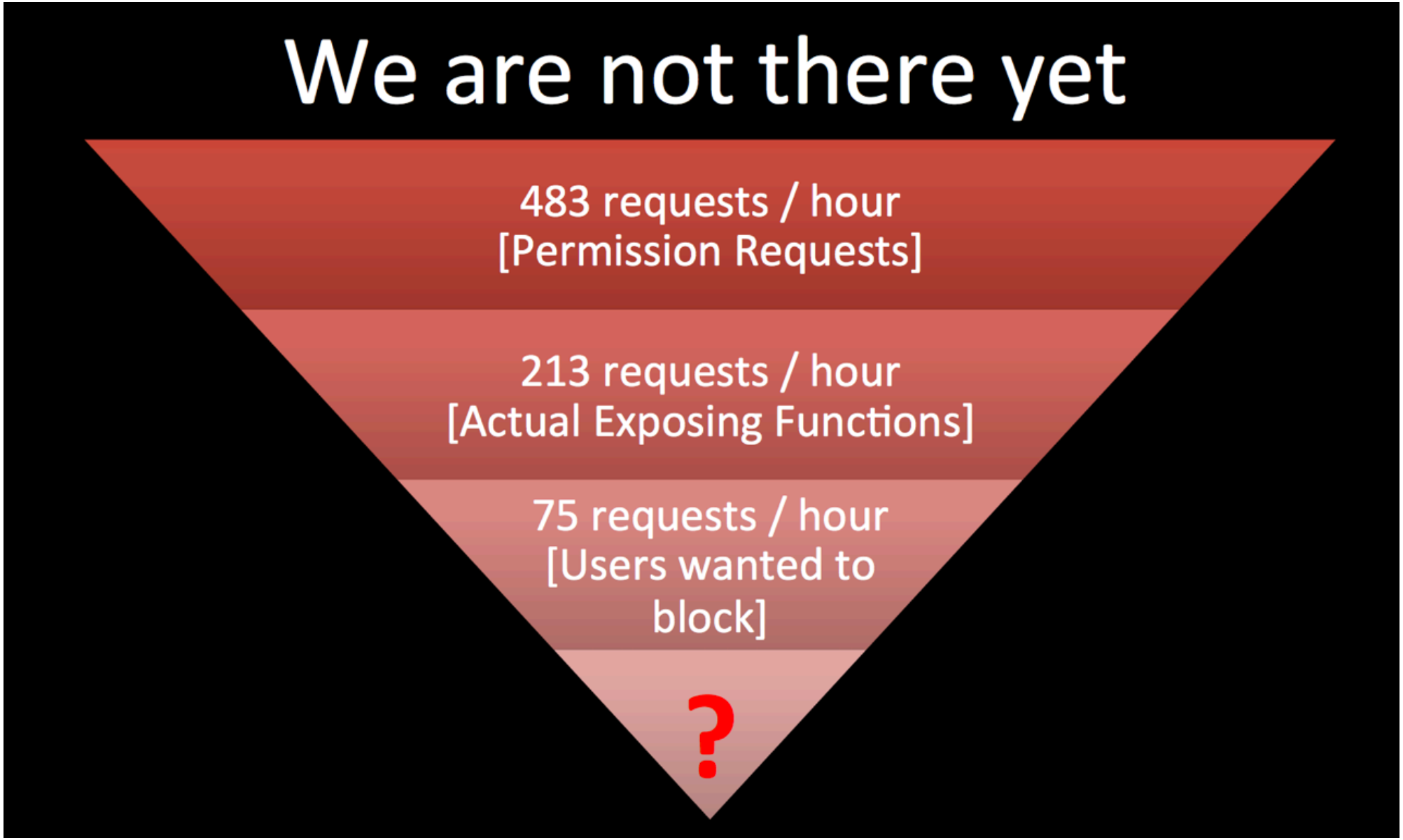
80% of users

would block at least one permission request.

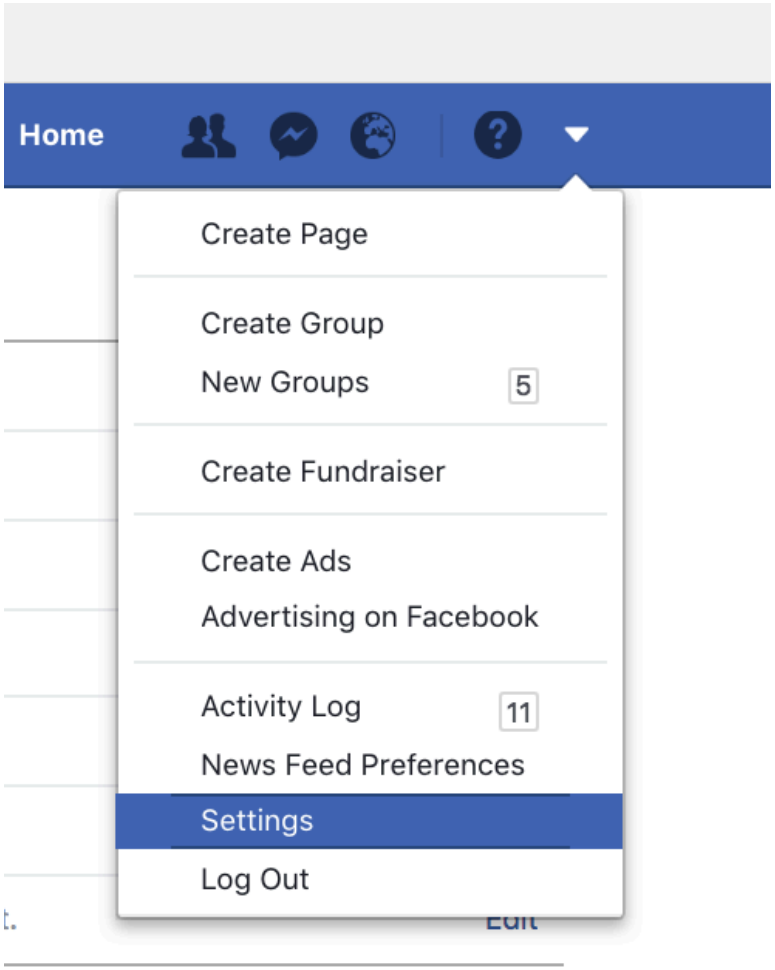
35% of all requests

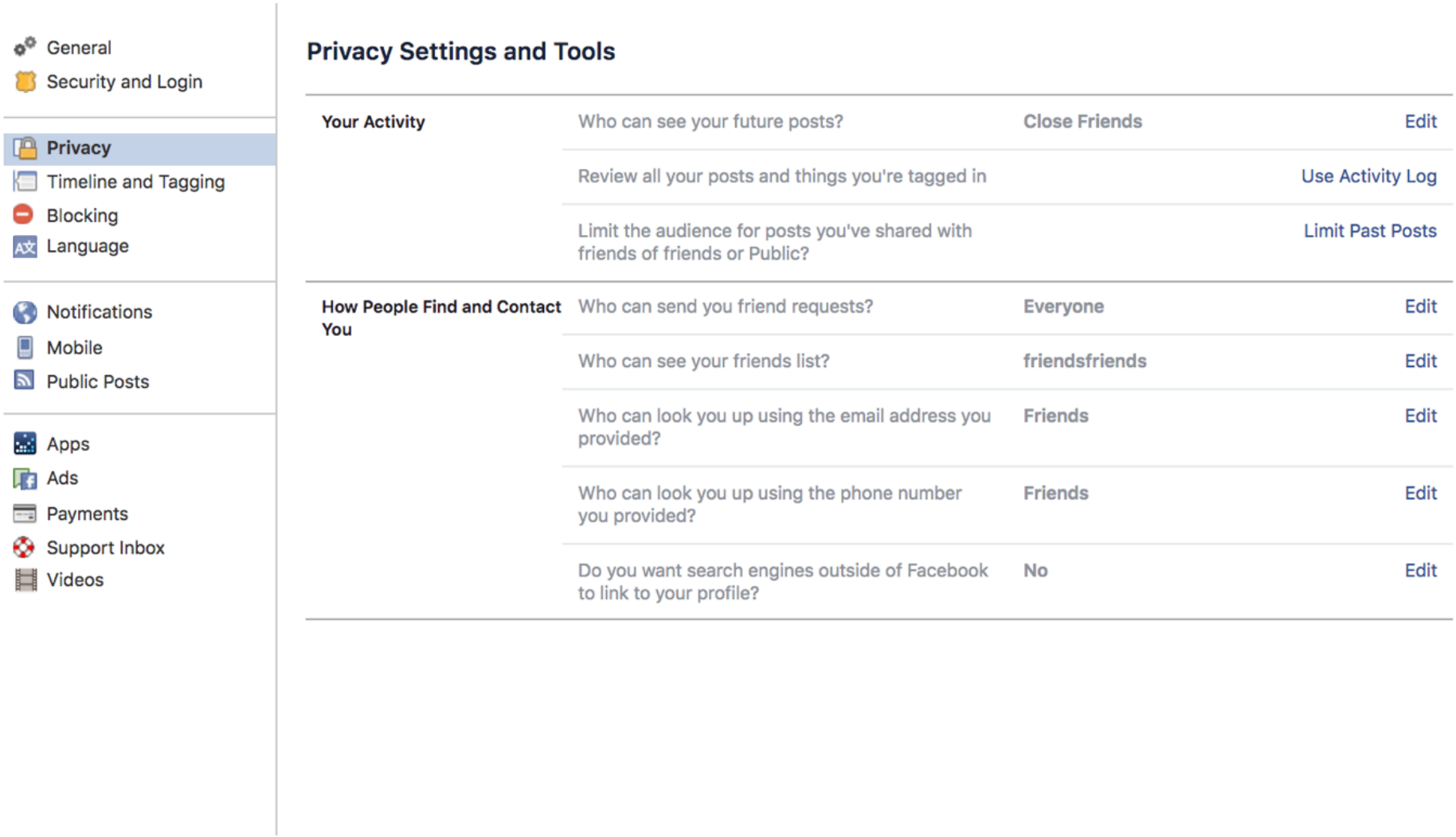
were deemed inappropriate.

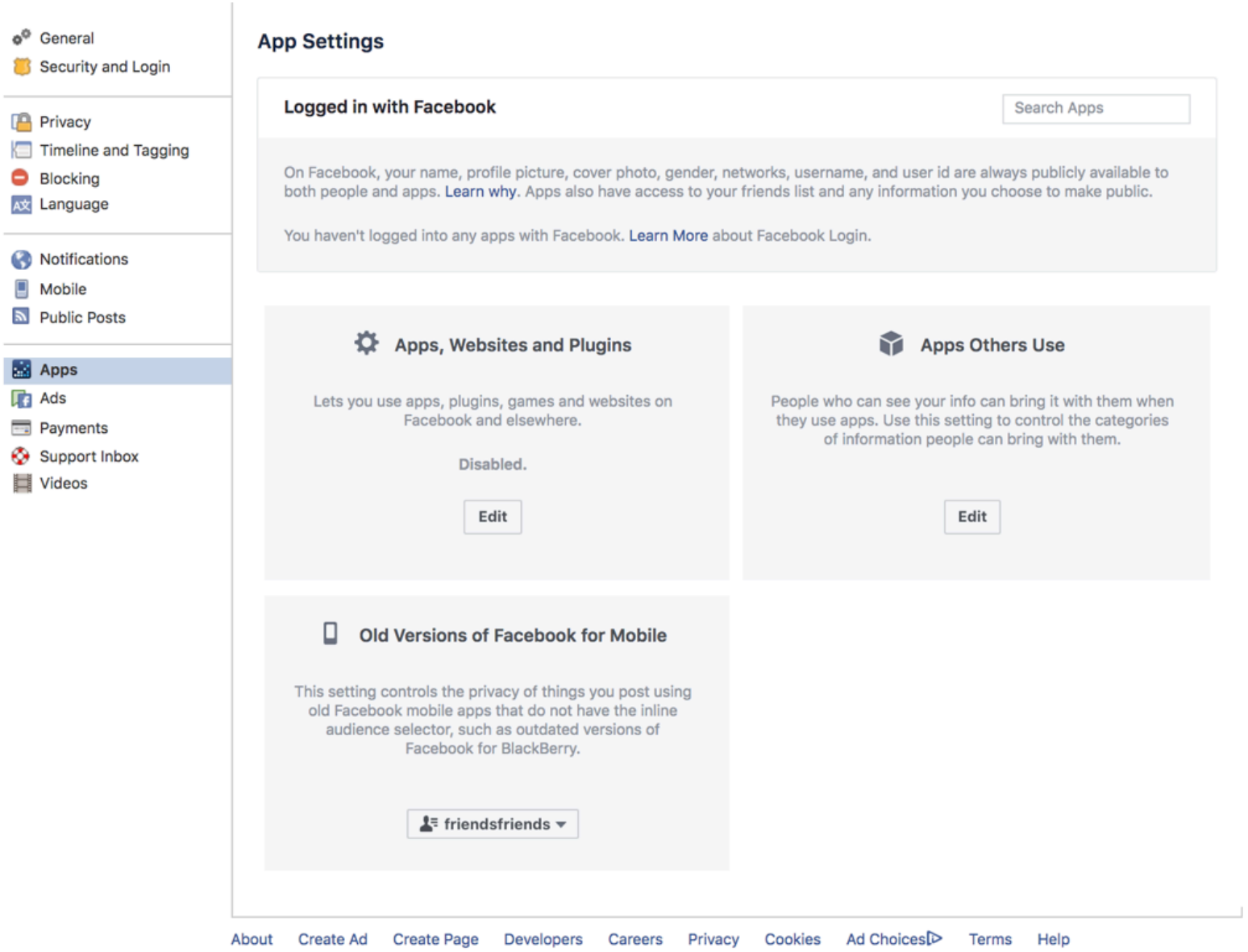
Android Permissions Remystified: A field study of Contextual Integrity (Wijesekera et al.)

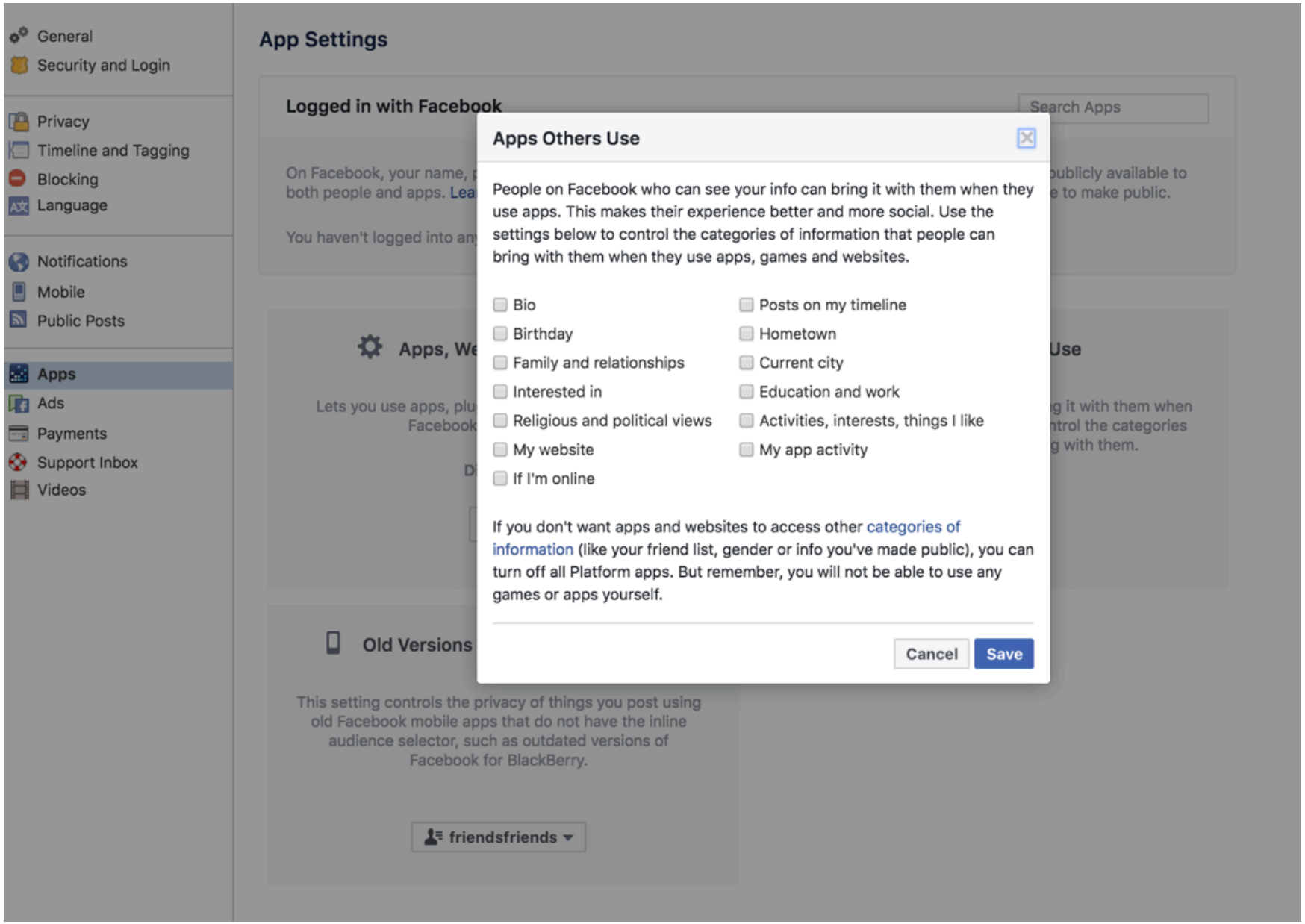


FB and CambridgeAnalytica




General
Security and Login
Privacy
Timeline and Tagging
Blocking
Language
Notifications
Mobile
Public Posts
Apps
Ads
Payments
Support Inbox
Videos
Privacy Settings and Tools
Your Activity
Who can see your future posts?
Close 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?
friendsfriends
Edit
Who can look you up using the email address you provided?
Friends
Edit
Who can look you up using the phone number you provided?
Friends
Edit
Do you want search engines outside of Facebook to link to your profile?
No
Edit


General
Security and Login
Privacy
Timeline and Tagging
Blocking
Language
Notifications
Mobile
Public Posts
Apps
Ads
Payments
Support Inbox
Videos
App Settings
Logged in with Facebook
Search Apps
On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available to both people and apps. Learn why. Apps also have access to your friends list and any information you choose to make public.
You haven't logged into any apps with Facebook. Learn More about Facebook Login.
Apps, Websites and Plugins
Lets you use apps, plugins, games and websites on Facebook and elsewhere.
Disabled.
Edit
Apps Others Use
People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.
Edit
Old Versions of Facebook for Mobile
This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.
friendsfriends
About
Create Ad
Create Page
Developers
Careers
Privacy
Cookies
Ad Choices
Terms
Help


General
Security and Login
Privacy
Timeline and Tagging
Blocking
Language
Notifications
Mobile
Public Posts
Apps
Ads
Payments
Support Inbox
Videos
App Settings
Logged in with Facebook
Search Apps
Apps Others Use
People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.
Bio
Birthday
Family and relationships
Interested in
Religious and political views
My website
If I'm online
Posts on my timeline
Hometown
Current city
Education and work
Activities, interests, things I like
My app activity
If you don't want apps and websites to access other categories of information (like your friend list, gender or info you've made public), you can turn off all Platform apps. But remember, you will not be able to use any games or apps yourself.
Cancel
Save
Old Versions
This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.
friendsfriends

DARK PATTERNS

Friend Spam ›

The product asks for your email or social media permissions under the pretence it will be used for a desirable outcome (e.g. finding friends), but then spams all your contacts in a message that claims to be from you.

Hidden Costs ›

You get to the last step of the checkout process, only to discover some unexpected charges have appeared, e.g. delivery charges, tax, etc.

Misdirection ›

The design purposefully focuses your attention on one thing in order to distract you attention from another.

Price Comparison Prevention ›

The retailer makes it hard for you to compare the price of an item with another item, so you cannot make an informed decision.

Privacy Zuckering ›

You are tricked into publicly sharing more information about yourself than you

Dark Patterns invoked in a case by the Norwegian Consumer Council

77. In particular, we request that Datatilsynet investigates and determines:

i. whether Google has a lawful legal basis to process the complainant's location data, particularly for those purposes related to advertising; and whether Google is properly informing the complainant about which legal basis the company uses to process her location data and for which purposes it is doing so,

ii. whether the conditions set out in Article 7 of the GDPR for valid consent are met, notably in those cases where Google may rely on consent as a legal basis for processing location data for advertising purposes;

iii. whether 'legitimate interests' constitutes an appropriate legal basis for the processing of location data carried out by Google in the context of the processing operations addressed by this complaint, notably in relation to advertising purposes.

iv. whether the design patterns and tricks used by Google to push consumers to share location data are compatible with the principles set forth in Articles 5.1 (a) and Article 25 of the GDPR regarding the fairness and transparency of processing and data protection by design and by default.

CNIL (French Data Protection Authority) already fined Google $50million Euros

Invalid Transparency and Information

The GDPR places much importance on companies informing users about how their data is used and what rights they have to intervene in the processing. Article 13 specifies information that must be disclosed to the user before any processing takes place, such as the nature and purpose of collection, and how long the data will be retained. Article 12 requires that this information be conveyed "in a concise, transparent, intelligible and easily accessible form." The aim is to ensure that users have control over what data is taken from them, and how it is used and shared.

The CNIL found that Google violated its duties of transparency and information. Specifically, Google obfuscated "essential information" about data processing purposes, data storage periods, and categories of personal information used for ads personalization. For example, the relevant information was "excessively disseminated" over multiple documents, and required users to click through five or six pages. Moreover, information was "not always clear" due to "generic and vague" verbiage. Yet the "massive and intrusive" scope and detail of the data collected by Google from its array of services and sources placed an increased obligation on the company to make its practices clear and comprehensible to users.

PRIVACY RESEARCH PARADIGMS

privacy as practice

- "the freedom from unreasonable constraints on the construction of one's identity" Agre
- improve user agency in negotiating privacy
- privacy integral to collective info practices
- aid in privacy decision making
- transparency of social impact

PRIVACY RESEARCH PARADIGMS

privacy as practice

"the freedom from unreasonable constraints on the construction of one's identity" Agre

enhance design of collective info practices

appropriate way to tag your colleagues?

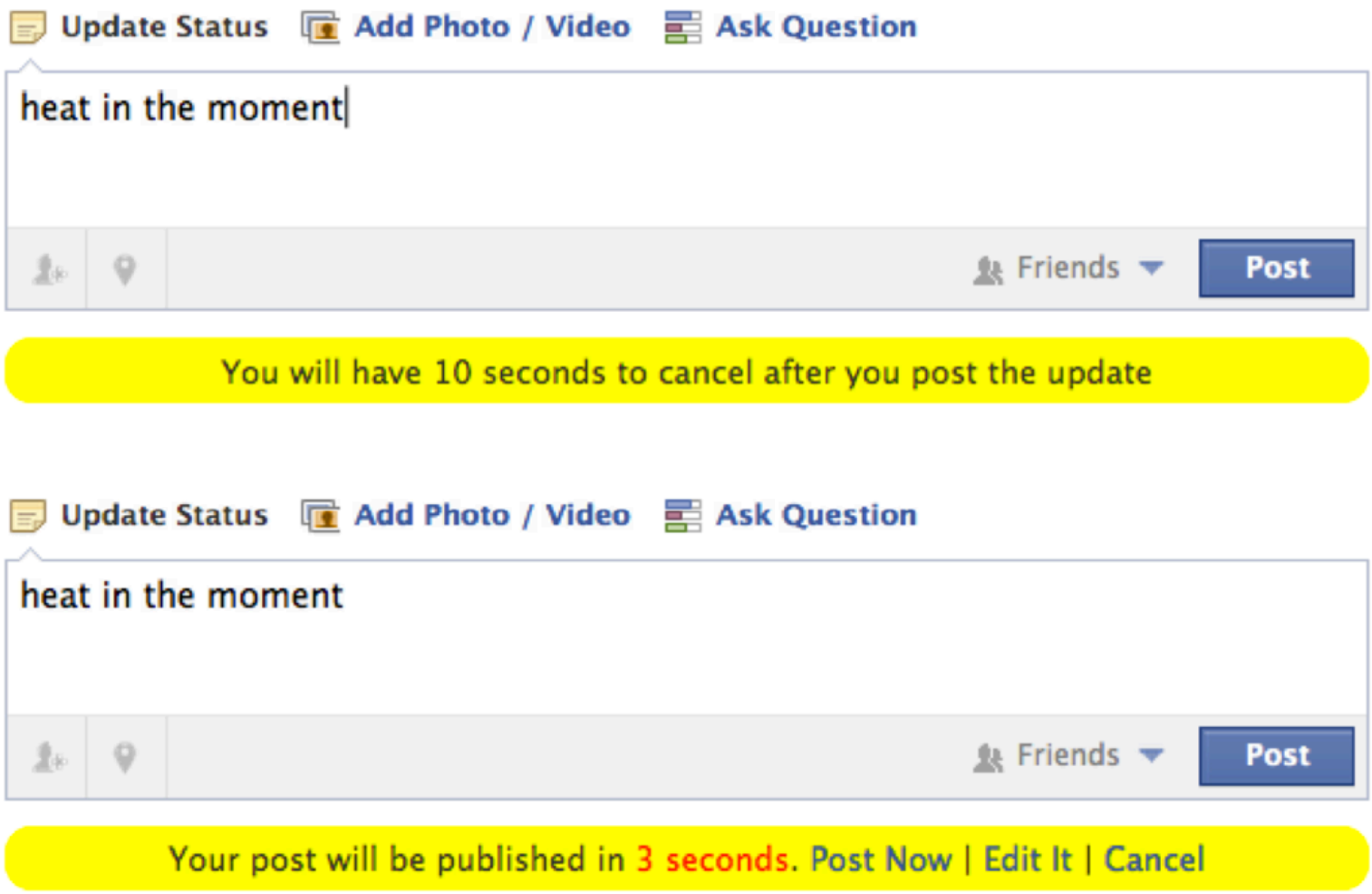
try different designs for tagging/ permissions/confirmations/removal

PRIVACY RESEARCH PARADIGMS

privacy as practice

feedback & awareness design

privacy nudges



slide: Lorrie Cranor

Shvartzshnaider et al., Crowdsourced, Actionable and Verifiable Contextual Informational Norms, Arxiv 2016.

Contextual Integrity:
actors
type of information
transmission principles

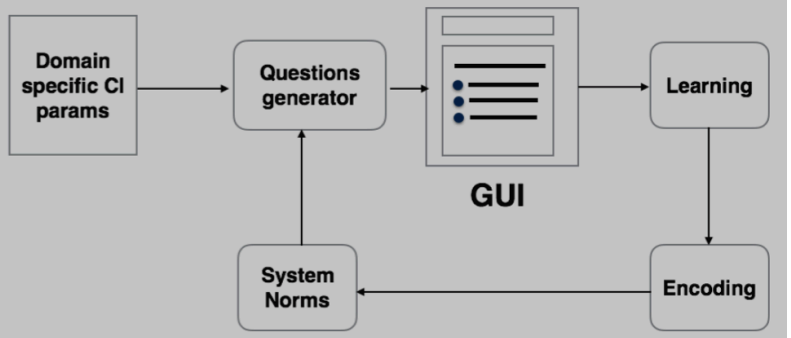
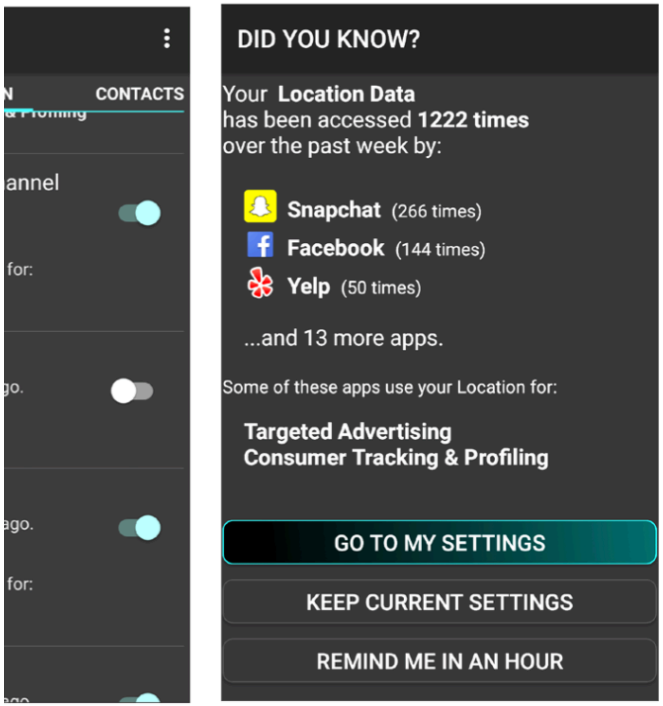


Figure 2: Our framework is designed to support several system states. The overall operation consists of 1) generating questions that correspond to information flows, 2) asking the questions, 3) deriving insights from the answers, 4) deciding on which set of actionable privacy rules (APR) to enforce, 5) generating questions from the enforced norms, 6) repeating by returning to step 2.

Liu et al., Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permission, USENIX, 2016.



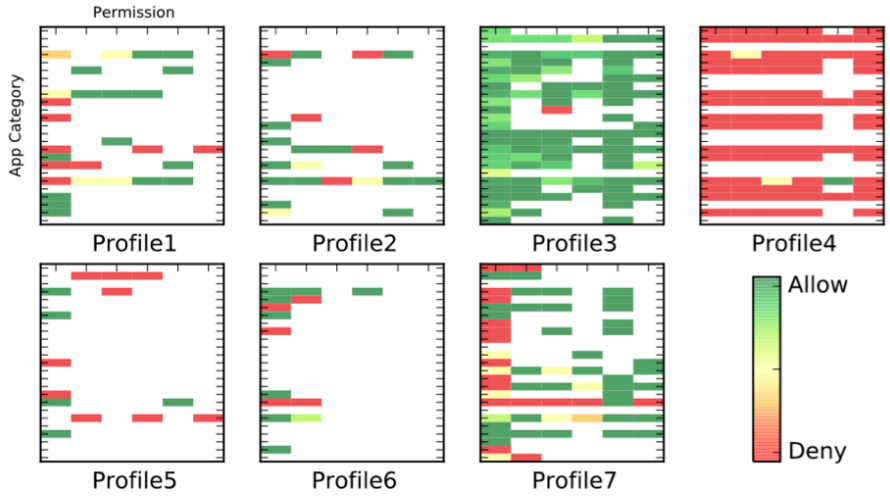


Figure 2: Privacy profiles learned from collected app privacy settings. Profile 1 is more protective on Location and Productivity apps than other profiles. Profile 2 denies phone call log permission more. Profile 3 is generally permissive. Profile 4 denies most permission requests. Profile 5 generally denies contacts, message, phone call log and calendar access, with only location and camera allowed for some apps. Profile 6 denies location and contact access of Social apps and Finance apps. Profile 7 is stricter regarding Social apps and location access in general.

PRIVACY RESEARCH PARADIGMS

privacy as confidentiality

privacy as control

privacy as practice

the paradigms are the basis of engineering privacy

- privacy as confidentiality: especially valuable in current data practices
- privacy as control: personal data-centric, likely to have great traction with GDPR
- privacy as practice: fundamental to smart environment and understanding user needs

privacy engineering requires rethinking software engineering

- ideally, all three approaches ought to be considered together
- good systems engineering includes privacy engineering
- privacy engineering will be important for GDPR compliance, too

thank you!

- Please contact me for further references
- f.s.gurses@tudelft.nl
- Interdisciplinary Summer School on Privacy
  - Theme: Dark Patterns
  - September 2.-6., 2019 Nijmegen, The Netherlands