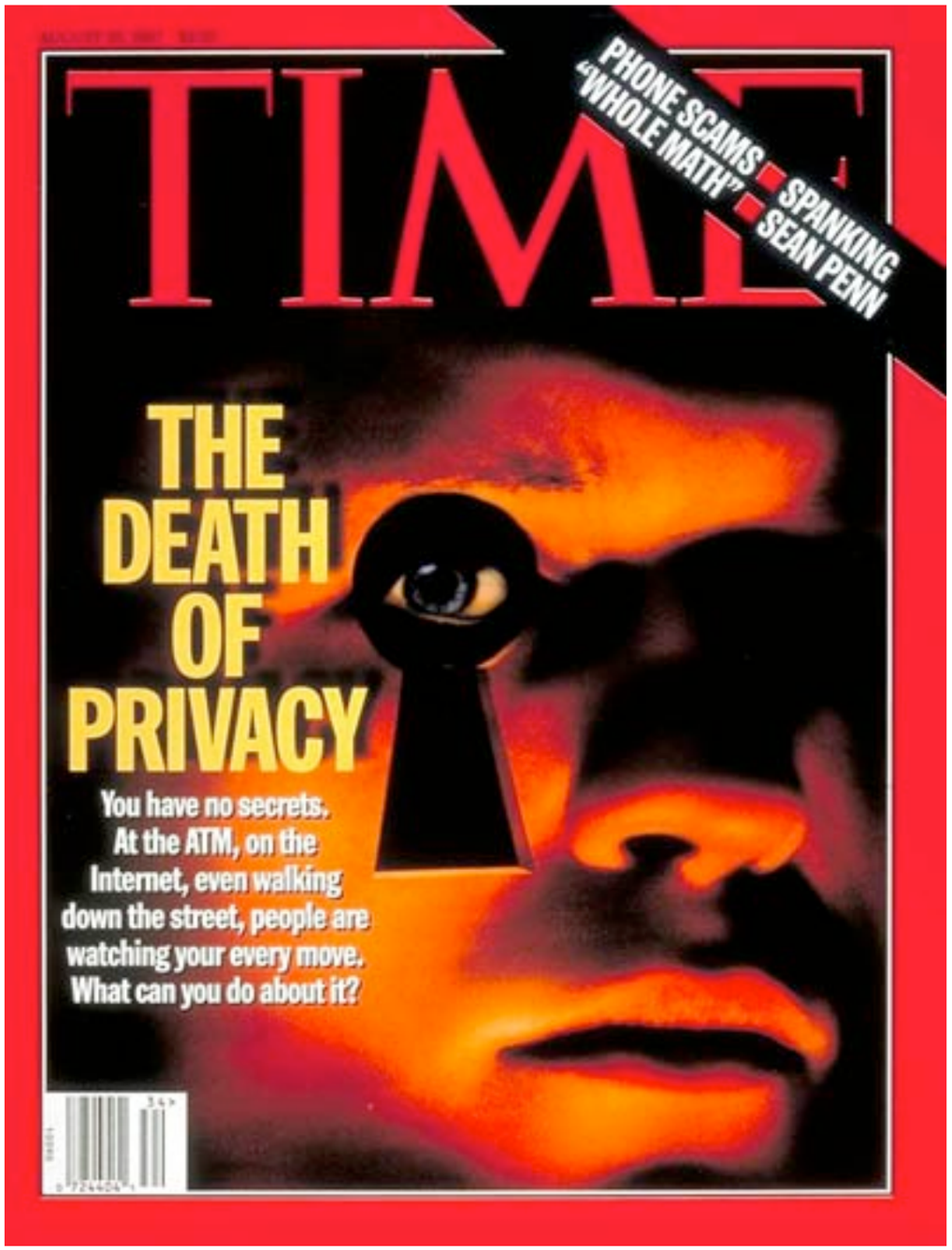
Privacy Research Paradigms in Privacy Engineering

Seda Gürses
seda_@ esat.kuleuven.be
COSIC, University of Leuven
CITP, Princeton University

28. Februar 2017
SecAppDev


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
goo.gl/fTyARu


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

getting privacy engineering right?

getting privacy engineering right?

privacy research

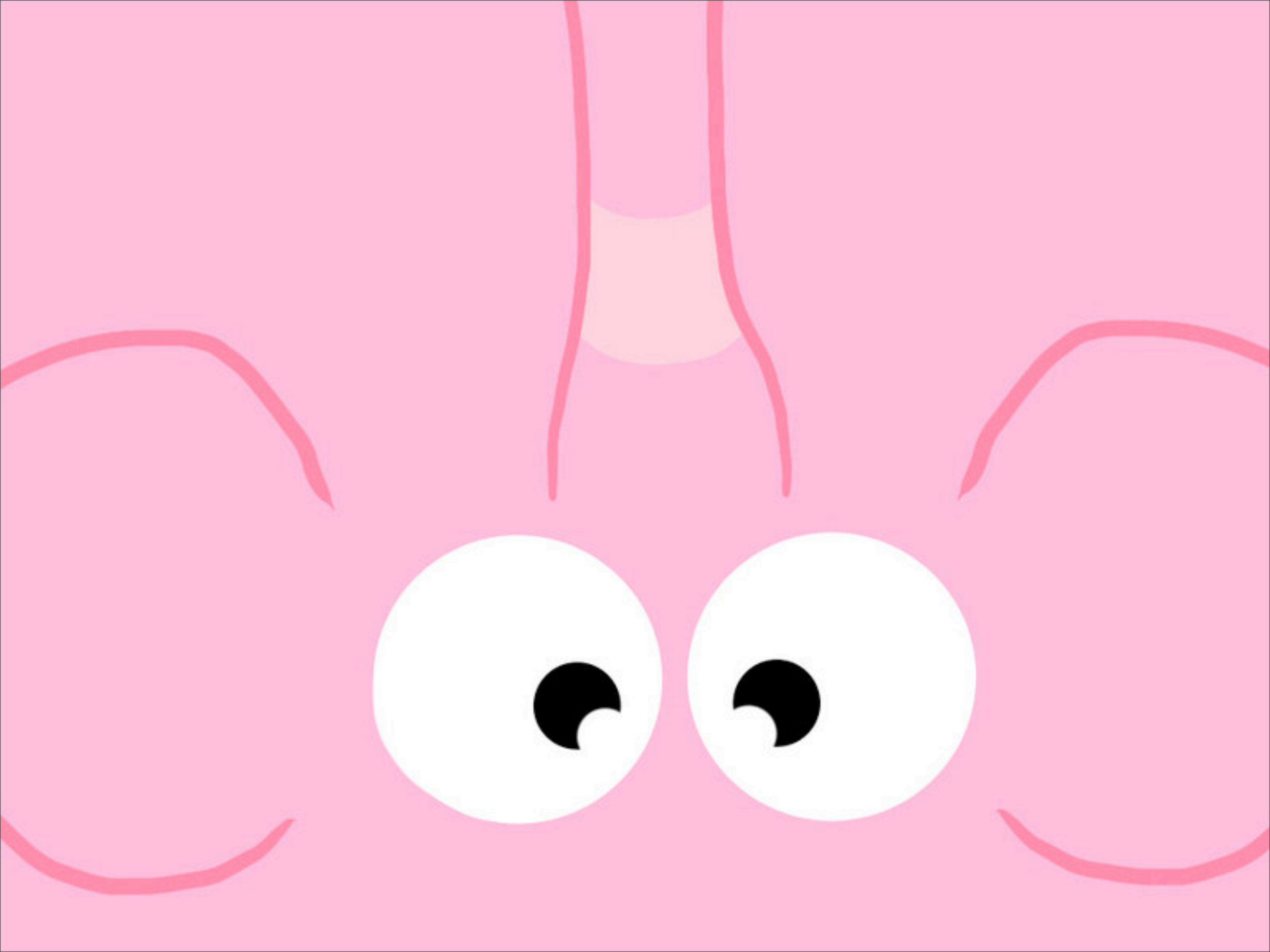
software engineering practice

privacy research

software engineering practice

privacy research

software engineering practice



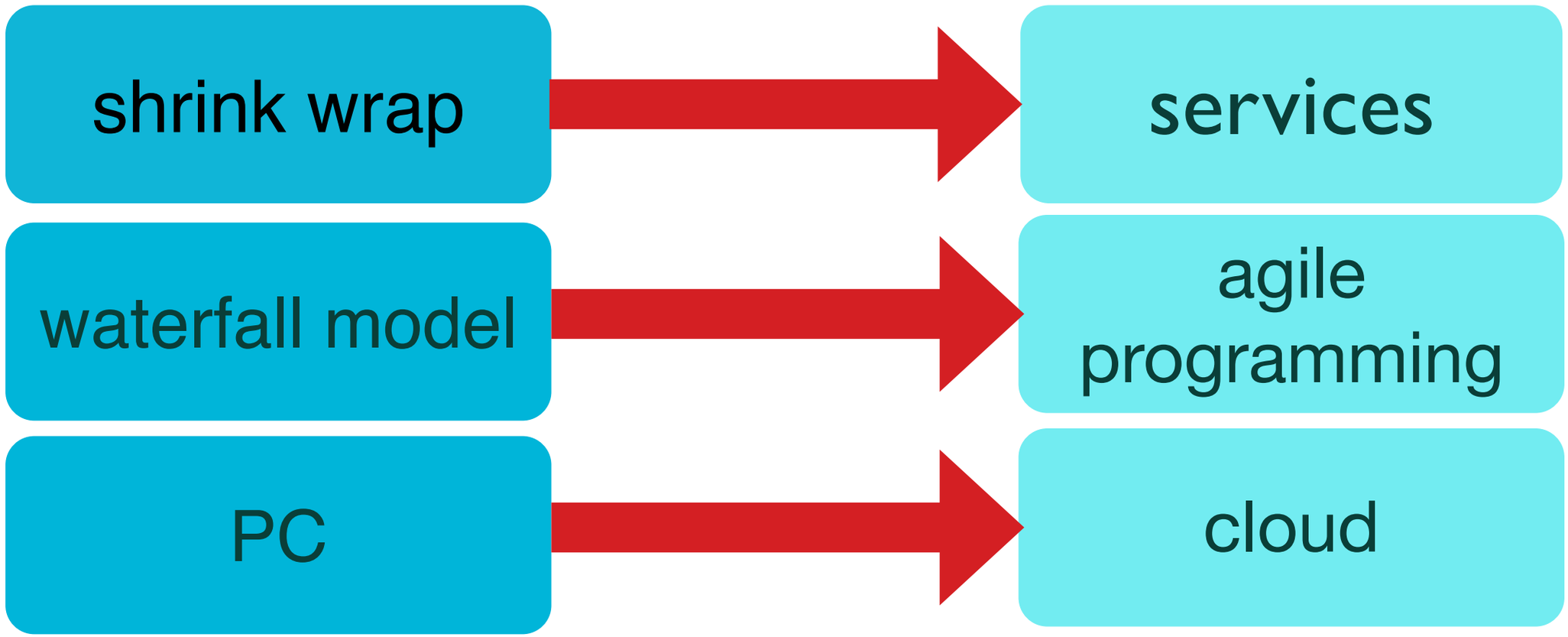
can it be that the practices around the production of software are an important element of privacy research?

privacy research

software engineering practice

matters?

the turn to agile



shrink wrap
software production

version
+
purchase

use

time

feature space

service bundle

pay per use

use

what is the impact of

the turn to agile in software engineering practice

on computer science research in privacy?

what is the impact of

the turn to agile in software engineering practice

on computer science research in privacy?

what is the impact of

the turn to agile in software engineering practice

on computer science research in privacy?

what is the impact of

the turn to agile in software engineering practice

on computer science research in privacy?

what is the impact of

the turn to agile in software engineering practice

on computer science research in privacy?

SOK
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

secure messaging

anonymous communications

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	✓	✓	✓	✗	✓	✓	✗

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

data protection/FIPPS compliance

transparency and accountability

individual participation and control

PRIVACY RESEARCH PARADIGMS

privacy as control

privacy policy languages

purpose based access control

Bell Group

information we collect	ways we use your information				information sharing	
	to provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt in		■	opt out	
cookies	■			■		
demographic information	■	opt in		■	opt out	
financial information						
health information						
preferences	■					
purchasing information	■	opt in		■	opt out	
social security number & gov't ID						
your activity on this site	■	opt in		■	opt out	
your location						

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

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

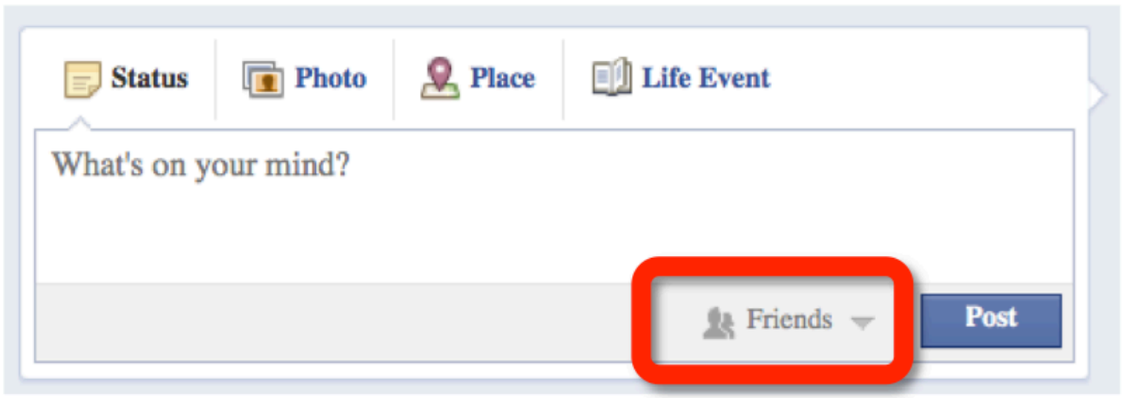
transparency of social impact

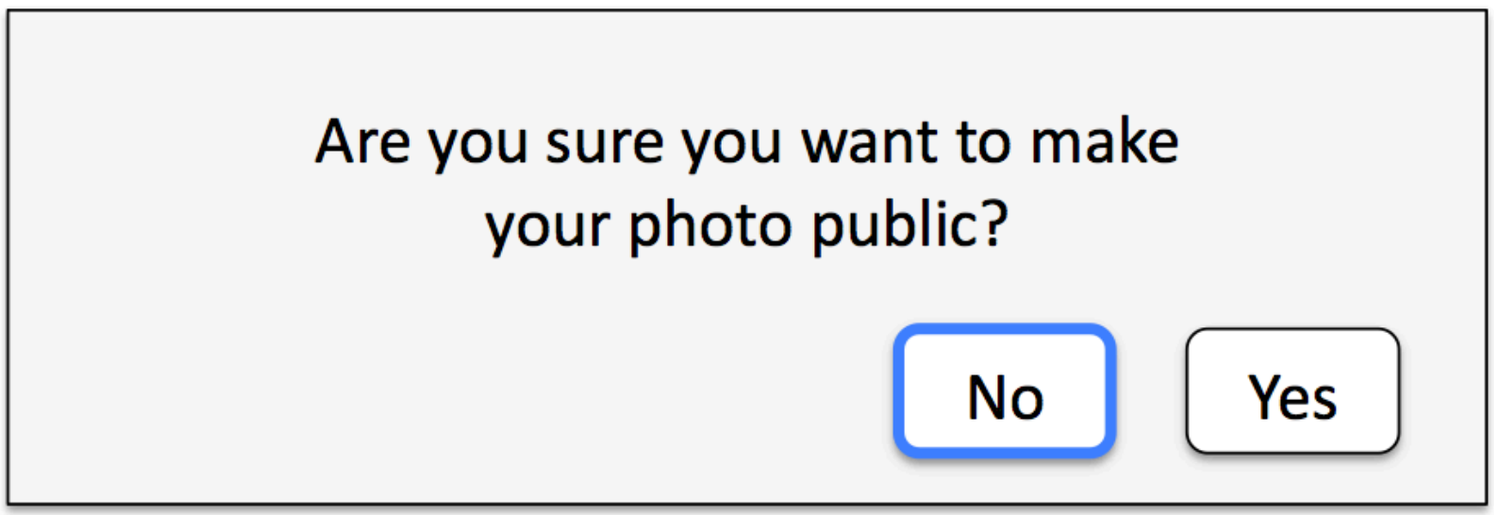
PRIVACY RESEARCH PARADIGMS

privacy as practice

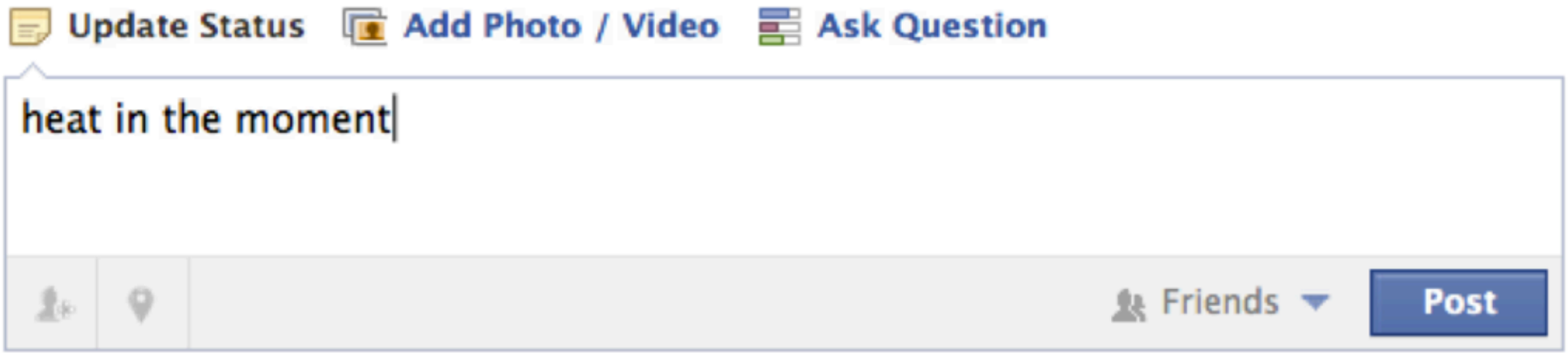
feedback & awareness design

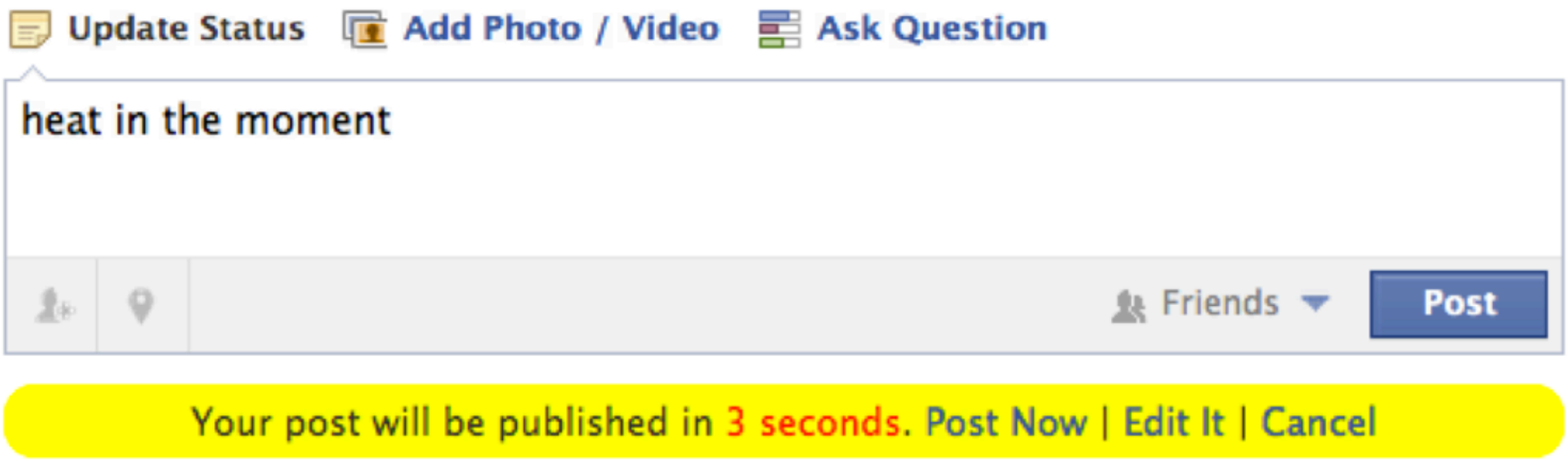
privacy nudges





slide: Lorrie Cranor





slide: Lorrie Cranor

PRIVACY RESEARCH PARADIGMS

privacy as confidentiality

privacy as control

privacy as practice

what is the impact of

the turn to agile in software engineering practice

on computer science research in privacy?

machine learning/AI and privacy

negative: undermine technical privacy protections?

positive: strengthen technical privacy protections?

co-evolution: how can we do ML/AI differently?

PRIVACY RESEARCH PARADIGMS

privacy as confidentiality

negative

website fingerprinting (Juarez et al., CCS 2014)

positive

obfuscation (location: Shokri, query:Nissenbaum)

anonymouth (McDonald et al., PETs, 2012)

co-evolution

differentially private recommender systems (McSherry et al, SIGKDD, 2009)

privacy preserving deep learning (Shokri & Shmatikov, CCS, 2015)

integrating PETs into agents, (Such et al., Knowledge Engineering Review, 2013)

PRIVACY RESEARCH PARADIGMS

privacy as control

negative

bypassing access control (PowerSpy, Michalevsky et al., USENIX, 2015)

positive

automatically analyzing privacy policies (Zimmeck, USENIX, 2014)

mining privacy goals from policies (Bhatia et al., TOSEM, 2016)

co-evolution

discrimination discovery, characterization and prevention (FATML)

A multidisciplinary survey on discrimination analysis
(Romei and Ruggieri, Knowledge Engineering Review, 2013)

PRIVACY RESEARCH PARADIGMS

privacy as practice

negative

facebook emotional contagion study
(Kramer et al. Proc. of National Academy of Sciences, 2014)

positive

improve privacy decision making and management
(Knijnenburg and Kobsa, TiiS, 2013; Lin et al., USENIX, 2014)

privacy agents

co-evolution

transparency through quantitative input influence (Datta et al. IEEE S&P, 2016)

explanatory debugging to personalize interactive machine learning
(Kulesza et al., ICIUI, 2015)

diversity in problems & solutions

integration

systematization

generalization

practice

privacy engineering

the field of research and practice that designs, implements, adapts and evaluates theories, methods, techniques, and tools to systematically capture and address privacy issues when developing socio-technical systems.

Gurses and Del Alamo, Privacy Engineering: Shaping an emerging field of research and practice, IEEE S&P, 2016.
http://vous-etes-ici.net/wp-content/uploads/2016/04/IEEESP_Pre.pdf

privacy theory

methods

techniques

tools

privacy theory

CONTEXTUAL
INTEGRITY

privacy theory

privacy

non-absolute

contextual

relational

opacity of the individual

data protection
FIPPs

procedural safeguards

accountability

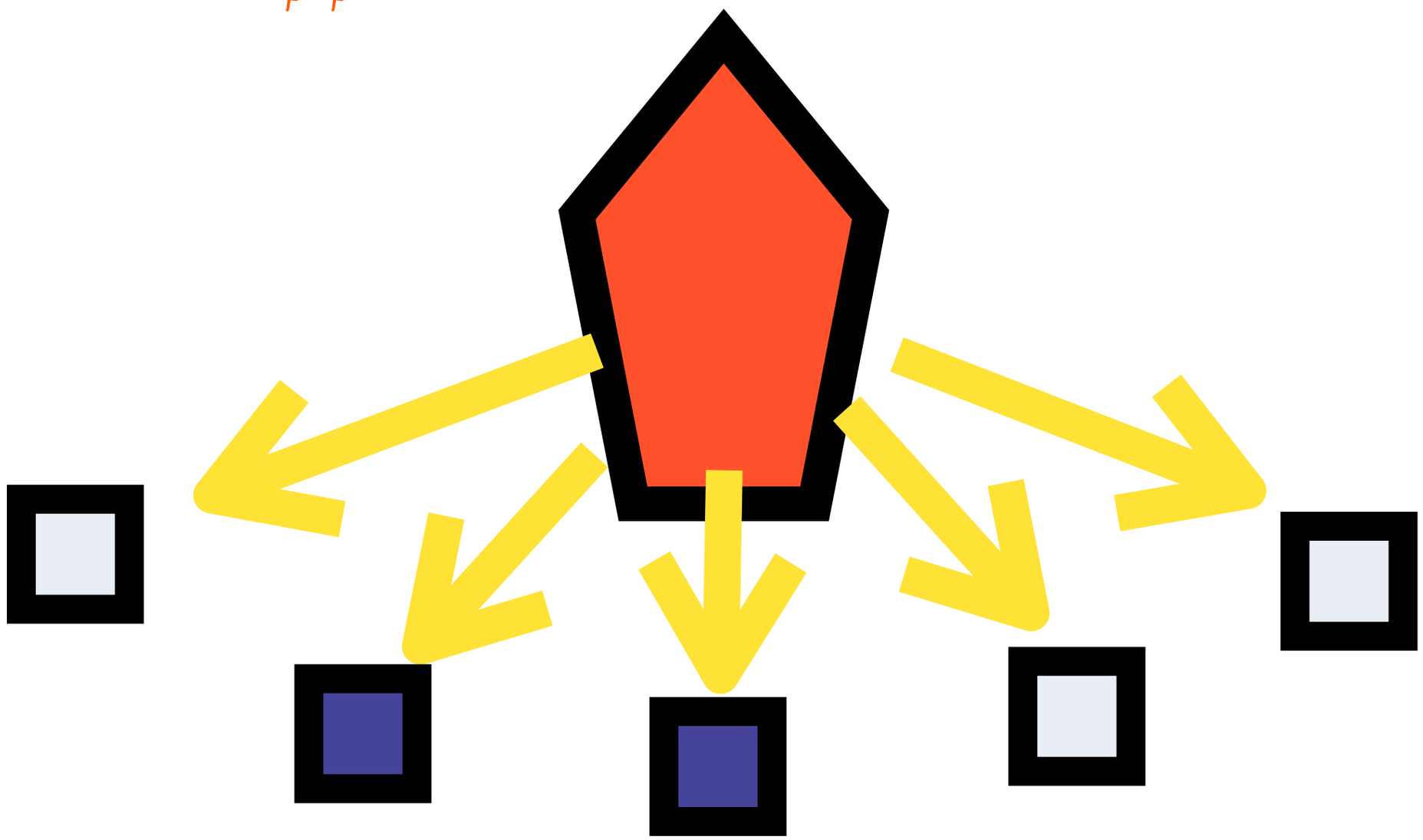
transparency

personal data

data minimization

privacy theory

Surveillance



privacy theory

methods

techniques

tools

methods:
approaches for systematically capturing and addressing privacy issues during information system development, management and maintenance

IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 35, NO. 1, JANUARY/FEBRUARY 2009

Engineering Privacy

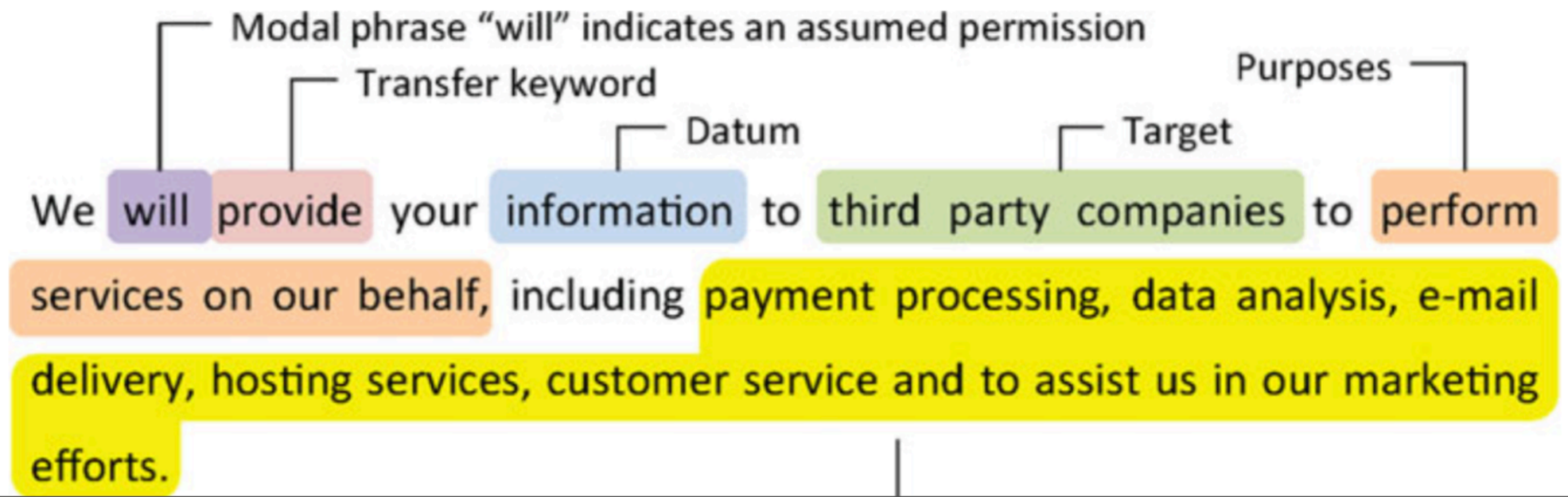
Sarah Spiekermann and Lorrie Faith Cranor, *Senior Member*, *IEEE*

Privacy stages	identifiability	Approach to privacy protection	Linkability of data to personal identifiers	System Characteristics
0	identified	privacy by policy (notice and choice)	linked	• unique identifiers across databases • contact information stored with profile information
1	pseudonymous		linkable with reasonable & automatable effort	• no unique identifies across databases • common attributes across databases • contact information stored separately from profile or transaction information
2		privacy by architecture	not linkable with reasonable effort	• no unique identifiers across databases • no common attributes across databases • random identifiers • contact information stored separately from profile or transaction information • collection of long term person characteristics on a low level of granularity • technically enforced deletion of profile details at regular intervals
3	anonymous		unlinkable	• no collection of contact information • no collection of long term person characteristics • *k*-anonymity with large value of *k*

techniques:
procedures, possibly with a prescribed language or notation, to accomplish privacy-engineering tasks or activities

Eddy, a formal language for specifying and analyzing data flow specifications for conflicting privacy requirements

Travis D. Breaux · Hanan Hibshi · Ashwini Rao



tools:
(automated) means that support privacy engineers during part of a privacy engineering process.

Tor Experimentation Tools

Fatemeh Shirazi
TU Darmstadt/KU Leuven
Darmstadt, Germany
fshirazi@cdc.informatik.tu-darmstadt.de

Matthias Goehring
TU Darmstadt
Darmstadt, Germany
de.m.goehring@ieee.org

Claudia Diaz
KU Leuven/iMinds
Leuven, Belgium
claudia.diaz@esat.kuleuven.be

Comparison

TECHNISCHE UNIVERSITÄT DARMSTADT

Metric	Shadow	TorPS	ExperimenTor
1. Size / number of relays	downscaling, simulation with 500+ relays possible	no downscaling	limited by available resources
2. Routing approach	not using additional weighting in node	ignoring paths being dropped due to	

socio-technical systems

standalone privacy technology

Tor/PreTP

privacy enhancement of system or function

privacy policy languages

research into privacy violations

web census

CONCLUSION

paradigmatically different privacy research within computer science

- Privacy engineering is the discipline that works on the gap between privacy research and software engineering
  - it is not about data management only
- Software engineering practice increasingly leans on machine learning and artificial intelligence
- The interaction of privacy and machine learning is a flourishing field
- The development privacy engineering methods, techniques and tools is instrumental for making this research actionable

thank you!

- Please contact me for further references
- seda AT esat.kuleuven.be