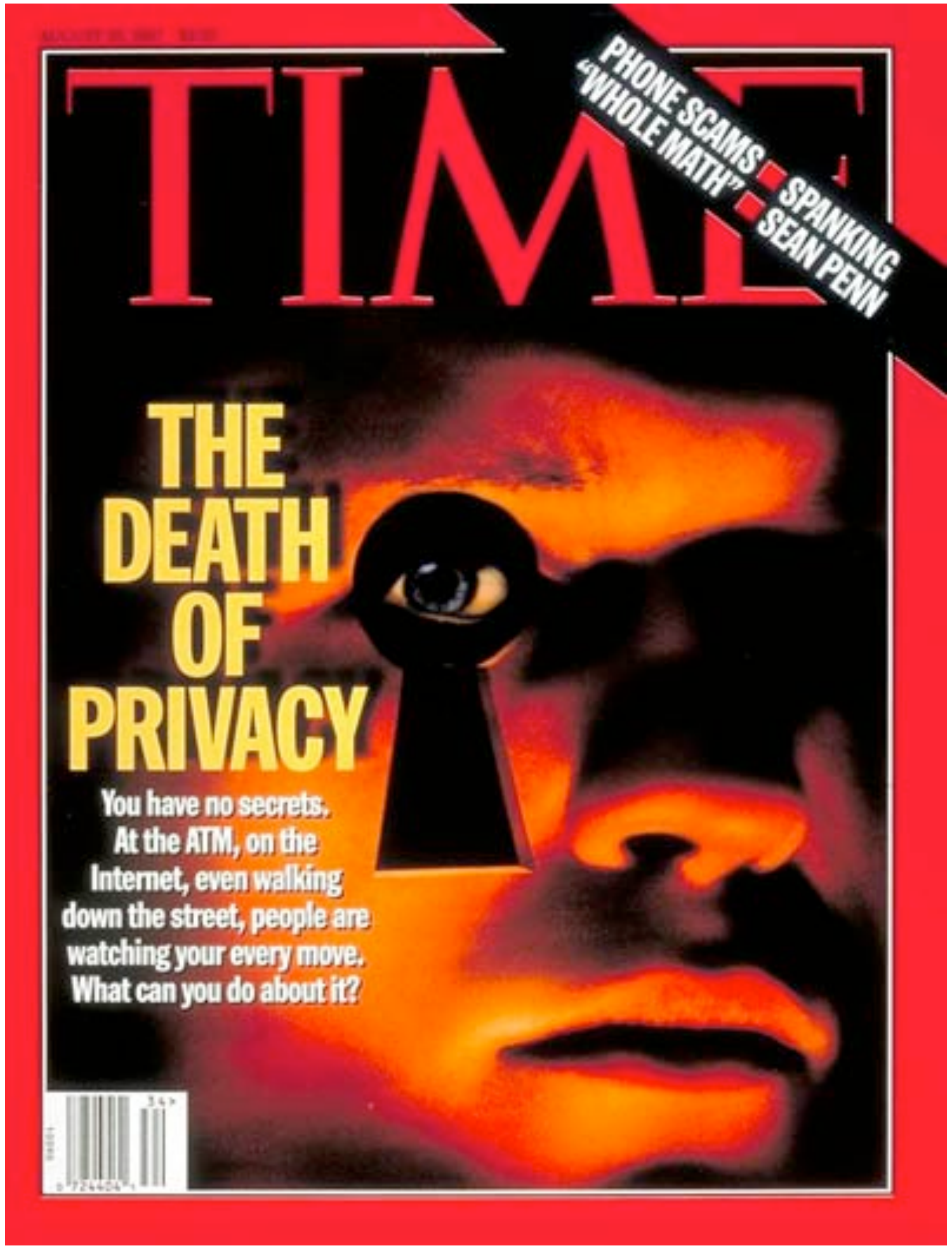
PET Semetary:
Privacy’s return from the dead and the Future of Privacy Engineering

Seda Gürses
CITP, Princeton University
COSIC, University of Leuven



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

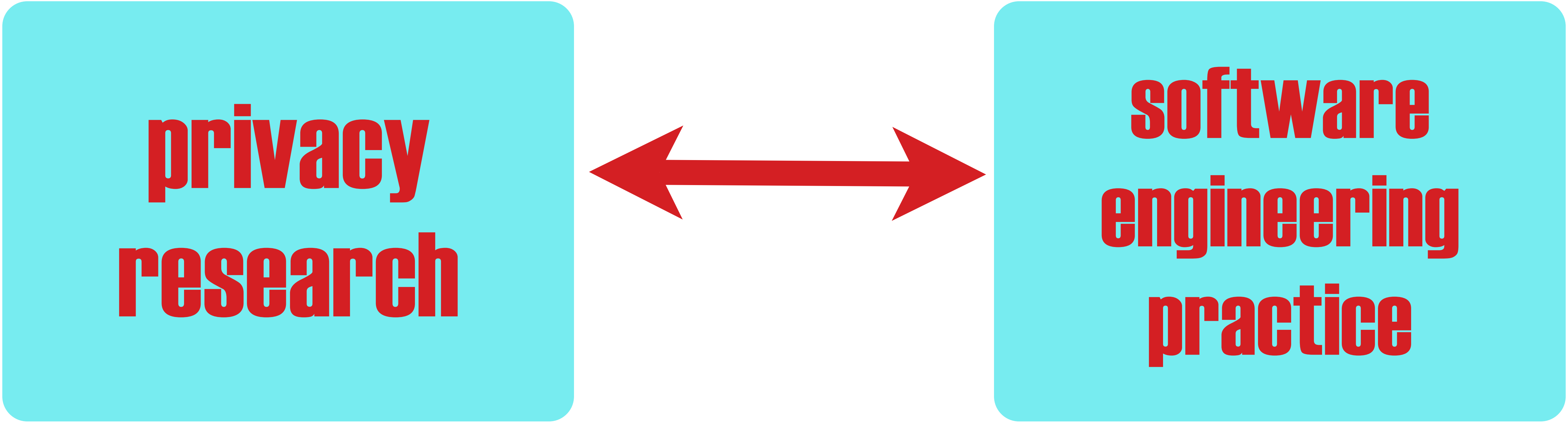
The End of PRIVACY

goo.gl/fTyARu
.1083-6101.2009.01494.x
PubMed ID19581585
http://scim.ag/1NNQB1Y
Longitude : -0.080152
053000196
Latitude
goo.gl/05qpy
Neiman Marcus
st-target

PET SEMATARY

getting privacy engineering right?

getting privacy engineering right?



privacy research

software engineering practice

PRIVACY RESEARCH PARADIGMS

privacy by architecture

privacy by policy

privacy by interaction

diversity in problems & solutions

integration

systematization

generalization

technical, legal, social practice

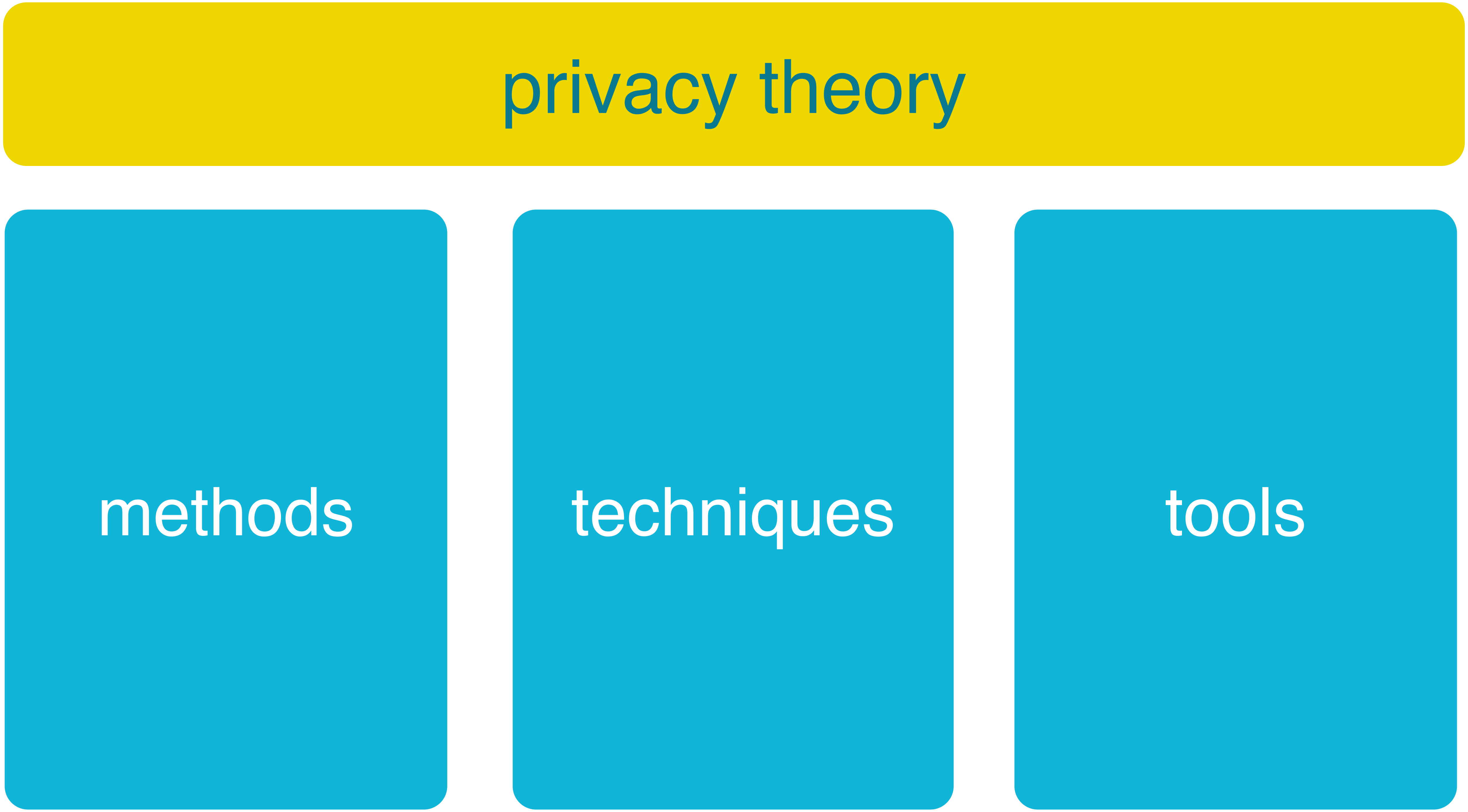
privacy engineering

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.

Privacy Engineering: Shaping an Emerging Field of Research and Practice
http://bit.ly/27Te955

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.



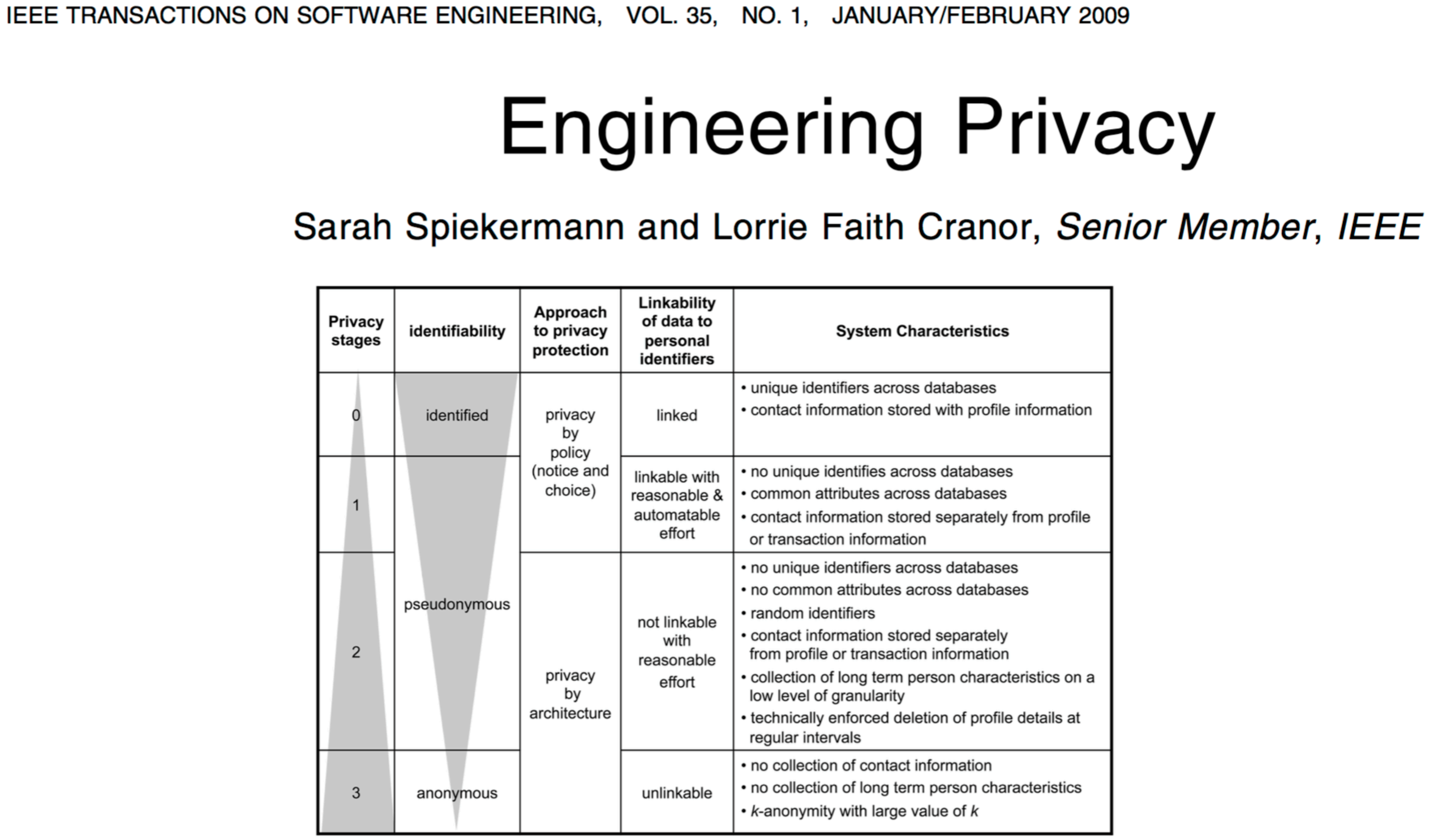
privacy theory

methods

techniques

tools

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



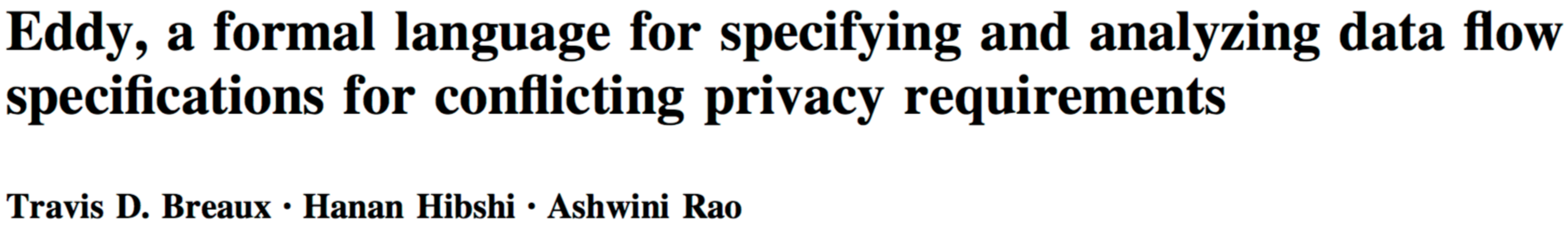
IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 35, NO. 1, JANUARY/FEBRUARY 2009

Engineering Privacy

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

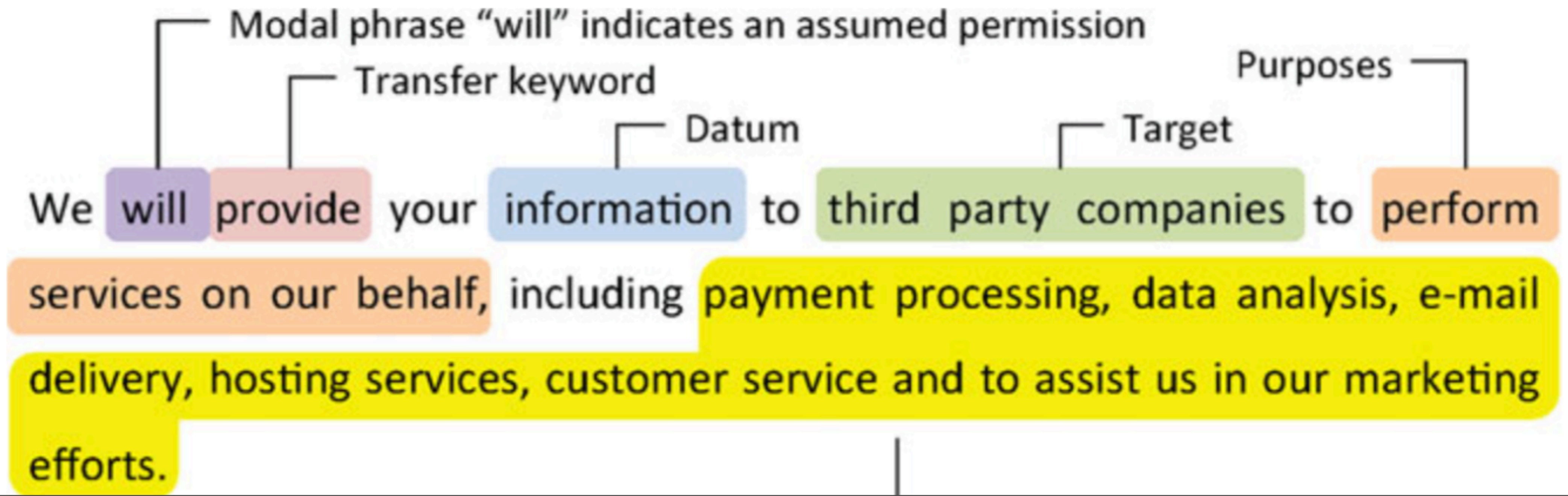
Privacy stages	identifiability	Approach to privacy protection	Linkability of data to personal identifiers	System Characteristics
0	identified	privacy by policy (notice and choice)	linked	• unique identifiers across databases • contact information stored with profile information
1	pseudonymous		linkable 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



We will provide your information to third party companies to perform services on our behalf, including payment processing, data analysis, e-mail delivery, hosting services, customer service and to assist us in our marketing efforts.

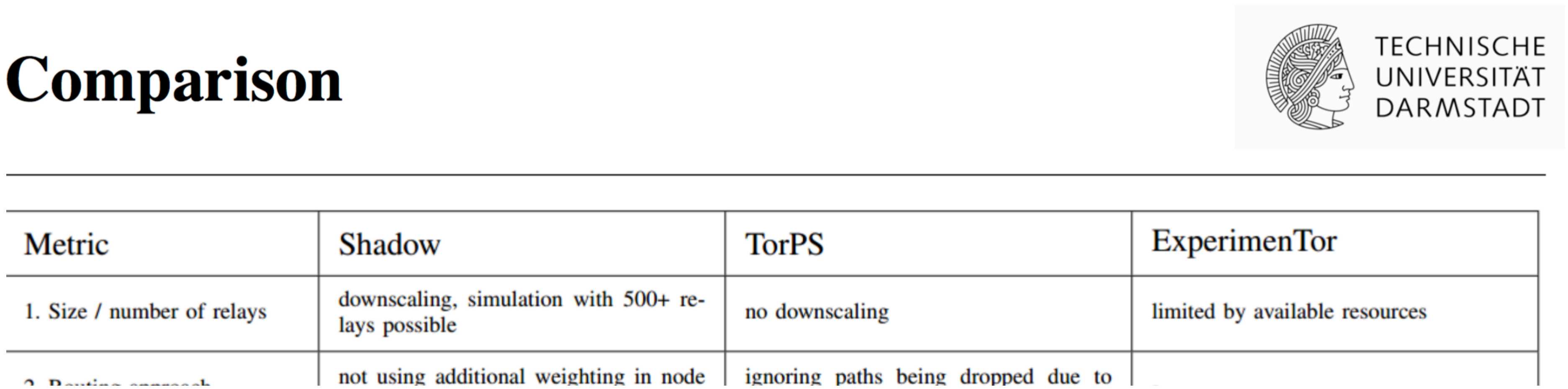
tools:
(automated) means that support privacy engineers during part of a privacy engineering process.

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



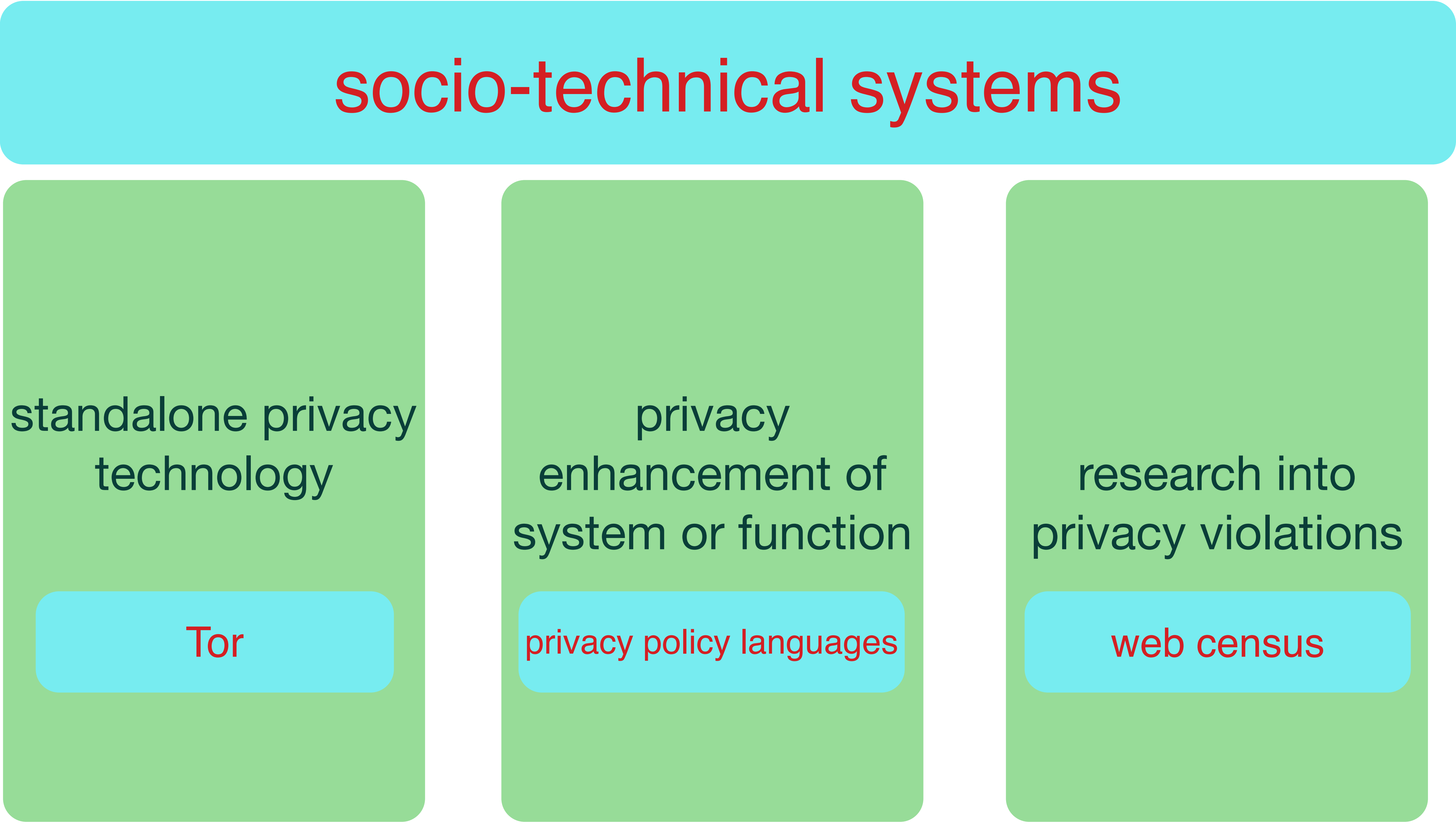
Comparison

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	

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.



socio-technical systems

standalone privacy technology

Tor

privacy enhancement of system or function

privacy policy languages

research into privacy violations

web census

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.

iwpe'15

empirical studies: how are privacy issues being addressed in engineering contexts?

machine learning and engineering: methods, techniques and tools to address privacy, fairness and semantic power

frameworks and metrics: for evaluating efficacy of privacy engineering methods, techniques and tools

help us define the field!!!

is the definition comprehensive?

does it address your current needs?

robust enough to capture your future challenges?

help our students!!!

Interdisciplinary Summer School on Privacy
https://www.pilab.nl/isp-summerschool-2016/

Nijmegen, iMinds, Princeton, PI Lab

Focus: Privacy in Service Architectures and Sharing Economy

Have a fun privacy problem for our students? Talk to me!

http://ieee-security.org/TC/SPW2016/IWPE/slides/case-study-template.pdf
http://bit.ly/1XyoJtr

thank you!

International Workshop on Privacy Engineering

http://ieee-security.org/TC/SPW2016/IWPE/

fgurses@princeton.edu

jm.delalamo@upm.es