Waseda University Brussels Office
早稲田大学ブリュッセルオフィス

Social Development of Secure and Privacy-enhancing Technologies

WORKSHOP SERIES



Tuesday 15 September 2026

ULB, Institute of European Studies, Av. Franklin Roosevelt 39– 1050 Bruxelles

WASEDA University

Workshop overview

This international workshop explores secure and appropriate approaches to managing personal data and digital identity in an era of widespread AI adoption.
In particular, the workshop focuses on the practical implementation and operation of digital identity systems and privacy-enhancing technologies (PETs) within existing legal and institutional frameworks, as well as the key challenges that arise in real-world settings.
Researchers from Japan and Europe will examine these issues from multiple perspectives, including technical design, legal frameworks, institutional practices, and human-centered considerations. The workshop combines invited talks with interactive discussions, with the aim not only of sharing current research insights but also of identifying common research challenges that may form the basis for future international collaborative projects.

SCHEDULE

Tuesday 15 September

09:30	**Registration**
10:00 – 10:10	**Opening** Kazue Sako, Waseda University Eri Anno, Waseda University Brussels Office
10:10 – 10:20	Self Introductions
10:20 – 10:50	**Session 1: Privacy Engineering** Frank Pallas (University of Salzburg) '*Privacy Engineering: From Principles and Technologies to Real-World Systems Integration and Trade-Offs*'
10:50 – 11:10	Coffee Break
11:10 –11:40	**Session 2: Privacy Protection in Digital Systems** Jaap-Henk Hoepman (Radboud University) '*Friction by Design (as a means to increase privacy and counter mass surveillance)*'
11:40 – 12:10	Laura Drechsler (KU Leuven) '*What's my age again?" Unpacking the Risk-Based Approach to Age Assurance in the GDPR*'
12:10 – 12:25	Session 2 Discussion
12:25–13:45	**Lunch**

13:45–14:15	**Session 3: Digital Identity and Privacy-Enhancing Technologies** Kazue Sako (Waseda University) '*A Design for Future Digital Identity Infrastructure in Japan*'
14:15–14:45	Yuriko Zemba (Waseda University) '*User Responses to Privacy-Enhancing Technologies: A Five-Country Study of Selective Disclosure*'
14:45–15:00	Session 3 Discussion
15:00–15:25	**Coffee Break**
15:25–15:55	**Session 4: Trustworthy and Privacy-Friendly AI Systems** Nicolò Romandini (University of Bologna) '*Trace, Account, Forget: Advancing Trustworthiness in Decentralized Machine Learning Systems*'
15:55–16:25	Meiko Jensen (Karlstad University) '*Data Subject Rights Engineering for Machine Learning Models: How to Manage your Digital Identity in the AI Era*'
16:25–16:40	Session 4 Discussion
16:40–17:25	**Wrap-up & Future Collaboration**
17:25–17:30	**Closing** Kazue Sako, Waseda University

Session 1: Privacy Engineering

Speaker Frank Pallas (University of Salzburg)

Title 'Privacy Engineering: From Principles and Technologies to Real-World Systems Integration and Trade-Offs'

Abstract:

Even though privacy-enhancing technologies (PETs) have reached a solid level of maturity and comprehensiveness, real-world systems and applications still don't properly materialize individuals' privacy needs. We suggest this to not stem from a lack of available computational primitives but from three main factors insufficiently considered in prevailing PET research:

1) an over-emphasis on anonymity and security with further privacy principles such as transparency or purpose limitation being largely overlooked,

2) a widespread lack of research dedicatedly exploring the integration into complex, distributed systems and respective development and operation practices, and

3) an insufficient comprehension of inevitable trade-offs, in the end often either materializing in an "all or nothing" aspiration for perfection or in hardly reproducible gut-level decisions.

The scene-opening talk will exemplarily illustrate how Privacy Engineering aims to overcome these factors through research subjects such as purpose-based data processing, so-called second-order non-functional properties of privacy technologies, or the experiment-driven examination of trade-offs between privacy, utility, and costs.

Session 2: Privacy Protection in Digital Systems

Speaker Jaap-Henk Hoepman (Radboud University)

Title 'Friction by Design (as a means to increase privacy and counter mass surveillance)'

Abstract

Digitisation owes its disruptive power to the near zero marginal cost of running digital services. Although the initial investment to create a digital service may be huge, creating a new digital copy, adding new users, or performing more work costs next to nothing. As a result, these services can scale up exponentially, creating all kinds of societal problems.

In particular, it creates opportunities for mass surveillance and widespread privacy infringements. For example, the careless design of a lawful access mechanism may allow for unfettered mass surveillance or the harassment of individuals, including minorities, vulnerable groups, political opponents, dissidents, and journalists.

Friction by Design studies mechanisms to significantly increase the marginal cost of running a digital service, to the point that adding a customer—or rather a target—becomes prohibitively expensive at some point. In a way, it aims to make the digital world behave more analogue, according to established laws of nature.

The presentation will discuss possible approaches and their limitations.

Speaker Laura Drechsler (KU Leuven)

Title '"What's my age again?" Unpacking the Risk-Based Approach to Age Assurance in the GDPR' (research undertaken in collaboration with Dr. Elora Fernandes and Prof. Simone van der Hof')

Abstract

Age assurance is increasingly required in digital environments, given the need to determine whether users are children when providing services that may affect their rights. The General Data Protection Regulation (GDPR) contains several requirements relevant to age assurance, notably concerning the validity of consent and its use as a mitigation measure within its risk-based approach.

The appropriateness of such measures depends, however, on the specific objectives pursued and the design of the methods applied. This paper analyses administrative decisions by European data protection authorities (DPAs) concerning age assurance methods implemented by digital services, identifying emerging criteria for assessing their appropriateness.

We find that these decisions provide limited guidance in practice, as DPAs often offer insufficient reasoning for why specific methods are considered appropriate or inappropriate, struggle to assess the state-of-the-art requirement under Article 25(1) GDPR, and insufficiently distinguish between different objectives of age assurance.

Session 3: Digital Identity and Privacy-Enhancing Technologies

Speaker& Organizer Kazue Sako (Waseda University)

Title 'A Design for Future Digital Identity Infrastructure in Japan'

Abstract

In this talk, drawing on my experience participating in expert committees at Japan's Digital Agency, Ministry of Health, Labour and Welfare, Financial Services Agency, Supreme Court, and National Police Agency, I identify a set of requirements and propose what I consider to be an ideal design for Japan's future digital identity infrastructure. I will discuss the current infrastructure surrounding the My Number Card and explore how this already valuable foundation can be further leveraged and extended to meet these requirements.

Speaker Yuriko Zemba (Waseda University)

Title 'User Responses to Privacy-Enhancing Technologies: A Five-Country Study of Selective Disclosure'

Abstract

Privacy-enhancing technologies (PETs) aim to protect users' personal information, but understanding how users respond to these technologies is also important for their

successful introduction. This talk focuses on selective disclosure, which allows users to reveal only the personal information needed for a particular transaction. We conducted a scenario-based survey experiment across five countries—China, France, Germany, Japan, and the United States—to examine how linkable and unlinkable selective disclosure affect privacy concerns and trust in data handlers. Unlinkable selective disclosure showed a broadly consistent tendency to reduce privacy concerns across countries, whereas the predicted cross-national differences in its effects were not supported. Trust responses were more complex. Among individuals less accepting of unequal power relations (those lower in power distance orientation), trust increased when the introduction of selective disclosure was considered, including when it was ultimately implemented. In contrast, among those more accepting of unequal power relations (those higher in power distance orientation), trust generally decreased when selective disclosure was considered but not implemented. Although the observed effects were modest, the findings suggest that while stronger privacy protection can reduce privacy concerns, trust responses may also depend on users' values and how they respond to decisions about technology introduction.

Session 4: Trustworthy and Privacy-Friendly AI Systems

Nicolò Romandini University of Bologna

Title 'Trace, Account, Forget: Advancing Trustworthiness in Decentralized Machine Learning Systems'

Abstract

Every week brings new breakthroughs in machine learning, with bold promises to transform critical domains such as healthcare, manufacturing, and mobility. Yet behind the growing excitement lies a difficult question: can we genuinely trust these systems? In distributed and decentralized environments, data often comes from unverified sources, contributors may act without coordination, and models evolve in ways that are difficult to monitor. While these solutions offer flexibility and scale, they also introduce serious risks. Without clear mechanisms for traceability and verification, machine learning models become vulnerable to poisoned data, unreliable updates, and subtle failures that may go unnoticed until it is too late. This talk invites a deeper look at what it means to build trust in learning processes from decentralized data sources. We will examine foundational challenges related to data provenance, participant authentication, and model accountability. We will explore how technologies such as distributed ledgers, decentralized identifiers, and verifiable credentials can guarantee integrity and transparency. In parallel, we will discuss algorithmic strategies to evaluate the influence of each data source, identify adversarial inputs, and enable targeted unlearning when necessary. This talk aims to raise awareness on some pressing problems and inspire a broader conversation on how to ensure that decentralized learning remains reliable, secure, and worthy of trust.

Speaker Meiko Jensen (Karlstad University)

Title 'Data Subject Rights Engineering for Machine Learning Models: How to Manage your Digital Identity in the AI Era'

Abstract

Informational self-determination, as the ability to manage one's own digital identity, is a fundamental cornerstone of privacy and data protection laws worldwide. However, when it comes to technical enforcement, these laws and the rights they provide to their data subjects become increasingly challenging to enforce.

With the advent of artificial intelligence, this arms race between policymakers and technological progress has intensified, leading to a plethora of unsolved challenges and conflicts between legal requirements and real-world AI systems.

In this talk, some of these challenges under the European GDPR will be highlighted, together with both the underlying issues and potential pathways for resolving them, from both a legal and a technical perspective, toward a privacy-friendly AI-driven future.

Waseda University Brussels Office

Avenue Antoine Depage, 1 - 1050 Brussels Belgium
https://www.waseda.jp/inst/brussels-office/news-en/

Contact:
Eri Anno
+32 476 538 320 eri.anno@ulb.be