

WORKSHOP: Bridging the Gap - Toward a Global Graduate Curriculum for Digital Privacy

Abstract. Digital privacy has emerged as a defining challenge at the intersection of technology, ethics, and society, yet graduate education has failed to keep pace. Privacy topics remain scattered across security courses, leaving professionals underprepared for specialized roles that regulation and innovation now demand. To address this gap, ACM, IEEE Computer Society, IEEE Digital Privacy Initiative, and IFIP have launched a global initiative to develop a unified Privacy Curricular Guideline. A Joint Task Force identified eight foundational knowledge areas - spanning technical, ethical, and applied dimensions. This workshop engages participants in a structured discussion to critically evaluate the framework, identify gaps, and contribute interdisciplinary perspectives on what a globally relevant privacy curriculum should encompass.

Keywords: Privacy Education, Digital Privacy, Privacy Body of Knowledge

1. Introduction

This year's Summer School theme - *Regulation and Innovation: Catalysts or Antagonists?* - names a tension nowhere more concrete than in privacy education. Regulatory frameworks are generating urgent demand for trained privacy professionals, while rapid technological change - generative AI, federated learning, decentralized identity - continuously reshapes what those professionals must know [1]. Yet no shared, globally recognized graduate curriculum exists to meet this demand [2].

To address this, ACM, IEEE Computer Society, IEEE Digital Privacy Initiative, and IFIP have launched a collaborative initiative to develop a **Privacy Curricular Guideline** for graduate programs. A global Joint Task Force first convened in December 2024 and reconvened in December 2025 to identify and refine eight foundational knowledge areas, now developed by dedicated Working Groups spanning institutions across North America, Europe and Latin America. The initiative engages IFIP's TC9 and TC11 communities, whose shared interests in security education, identity management, and the technical and societal dimensions of data misuse are woven throughout the framework.

Privacy topics are currently fragmented across security courses, leaving graduates ill-prepared for the specialized roles - privacy engineer, data ethicist, privacy officer - that regulation and industry increasingly demand [3]. A dedicated curriculum fills that gap: one grounded in user autonomy, data governance, and ethical responsibility, and built on the recognition that privacy and identity are technically and institutionally inseparable. This workshop invites participants- the next generation of educators and curriculum designers - to engage critically with the framework, challenge its assumptions, and bring perspectives from their own disciplinary and cultural contexts.

2. Privacy Curricular Framework

The Joint Task Force identified eight knowledge areas that together define the scope of graduate-level digital privacy education:

- **Grounding Privacy Discipline.** Core concepts, privacy as a human right, ethical frameworks, normative theories, and standardized terminology [4].

- **Privacy Foundations.** Trends in ICT, mental models of privacy, measuring privacy, building privacy-respecting systems, and digital identities.
- **Foundational Computing Concepts.** Networking, data storage & analytics, systems considerations, secure concepts in coding, access control, ML/AI, and cryptographic primitives.
- **Privacy Preserving/Enhancing Techniques.** Homomorphic encryption, differential privacy, federated learning, secure multi-party computation, secure architecture design, privacy-aware user interface design, and anonymization.
- **Information and Communication Systems.** Data protection across lifecycle, protecting data processing/computations, privacy in smart/ubiquitous environments, privacy governance, risk management, and privacy usability.
- **Privacy Development Lifecycle.** Privacy DevOps, privacy requirements, privacy impact assessments, privacy threat modeling, Privacy by Design, and privacy assurance.
- **Applied Domains.** Sector-specific challenges in energy, healthcare, finance, government/public services, digital wallet, and connected vehicles.
- **Privacy-Related Industry Perspective[s].** Emerging privacy roles & skillsets, privacy operations, privacy interoperability, and standardization.

3. Planned Activities

The workshop will be highly interactive, combining concise presentations with facilitated small-group discussions to collaboratively advance a global privacy curriculum.

Framing (15 min). A brief opening presentation on the state of privacy education globally, the initiative's progress, and the eight knowledge areas. Participants are invited to reflect on gaps in their own graduate training.

Small-Group Discussion (50 min). Groups are each assigned one or two knowledge areas and asked to: (a) evaluate scope and learning outcomes for graduate-level appropriateness; (b) identify gaps, overlaps, or missing topics; and (c) consider how regional regulatory context should shape each area's treatment.

Plenary Synthesis (25 min). Groups report key findings, and a facilitated discussion surfaces shared themes and productive disagreements.

4. Outcomes and Continued Engagement

The workshop will produce a short proceedings paper documenting key arguments, points of convergence, and open questions - feeding directly into the next iteration of the curricular framework. Participants who wish to continue contributing will be invited to join one of the initiative's Working Groups, offering a concrete pathway to shape a standard that will influence how digital privacy is taught worldwide.

References

1. Gürses, S., Del Alamo, J.M.: Privacy engineering: Shaping an emerging field. *IEEE Security & Privacy*, 14(2), 40-46 (2016)
2. Steinhagen, D., et al.: An inventory of privacy curricula in higher education. *Information Systems Education Journal*, 19(3), 21-30 (2021)
3. IAPP and EY: Privacy in Higher Education Report (2022). <https://iapp.org>
4. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press (2009)