Global Digital Foundation
The Digital Policy Network

Foundation Forum 21
Regulation, Innovation, Standards

AI Security & Privacy

7 December 2021 | Brussels

CEPS · ECLIPSE FOUNDATION · ETSI The Standards People · techeu · HUAWEI

One impact of the Covid-19 pandemic in Europe has been a step change in digital transformation affecting all sectors. Industries from pharmaceuticals to manufacturing, and services have begun to build an enabling foundation for the digital society. As digital technologies increase productivity, improve energy efficiency and uncover new business models, EU and member-state governments are looking to develop new regulations to guide this journey.

The European Commission has prioritized legislation to regulate emerging technologies, including Artificial Intelligence through the Artificial Intelligence Act, the upcoming Data Act, as well as through facilitating the creation of European data spaces in specific sectors (Health, Transportation).

In order to progress the dialogue around a shared responsibility for AI, Huawei is supporting the Foundation Forum 2021, an initiative focused on developing standards of AI security & privacy across the AI supply chain chaired by **Global Digital Foundation**. The Foundation Forum 2021 will feature three workshops moderated by **CEPS, Eclipse Foundation** and **ETSI**. These will focus on the role of AI regulation, technology, cybersecurity and privacy standards in enabling AI innovation and data governance in Europe. With a diverse group of stakeholders across different sectors, attendees will benefit from a wide range of discussions through a convention of key stakeholders.

Why should these organisations lead the conversation?

The discussions are moderated by CEPS, Eclipse Foundation and ETSI with academics, SMEs and industry partners to share their learnings about how regulation, innovation and standards can be applied to realize digital transformation. CEPS is at the forefront of leading the policy discussion around AI security and proposing policy recommendations through the Task Force on AI Report. Eclipse Foundation brings together an innovative industry ecosystem promoting Open Source and industry collaboration. ETSI is a leader in setting futureproof standards for Secure AI.

Why is there a need for a technical, practical focus?

AI use cases from European SMEs and Industry organisations are embedded into the panels so that policymakers and regulatory authorities are updated about how technology is also being utilized to enable new opportunities and address regulatory concerns. Global tech companies have long followed the EU's lead and embraced privacy and security laws like the General Data Protection Regulation (GDPR). Europe's values and regulatory leadership on technology policy are being adopted by governments around the world, while tech companies also implement privacy and security by design in integrated product development roadmaps.

This is why it is important for policymakers to ensure that a shared responsibility for AI is written into regulatory frameworks to help create the right conditions for businesses and consumers to enjoy the benefits of AI innovation.

Attendees at the Foundation Forum 2021 will include:

- Policy organisations
- Cybersecurity agencies and organisations
- EU institutions
- Industry SME and enterprises
- Standards organisation

What will be the outcome of these panels?

The panels will aim to contribute to the policy discussion around cybersecurity in AI, supply chain security as well as sharing insights on combating potential malicious uses of AI from a cybersecurity are shared across the ecosystem.

The panel discussions will be preceded by a keynote speech and followed by a closing session that will summarize discussions held throughout the day. To support any challenges with travel due to Covid-19 or other conflicts the event is been organized as a hybrid forum to support attendees who are unable to physically attend via dial-in through secure virtual video conferencing. The intent for the Forum is for all the speakers to be present to maximize this interactive discussion and networking opportunity.

13:30 **Registration Open**

13.58 **Opening Remarks** (5 min)
Paul MacDonnell, Executive Director, Global Digital Foundation

14.02 **Keynote speech** (15 min)
MEP Brando Benifei

14.20 **Keynote speech** (15 min)
MEP Tsvetelina Penkova

14.35 **Break** (5 min)

14.40 **Topic 1:**
AI Innovation & Regulatory Frameworks in Europe (50 min)
Moderated discussion by Lorenzo Pupillo, Associate Senior Research Fellow and Head of the Cybersecurity Initiative, CEPS

The first panel discussion will focus on how the EU's new Artificial Intelligence Act, as well as other horizontal and sectoral legislation will impact industry in Europe. Each panellist will provide a unique perspective, and the discussion will be opened and moderated by CEPS who has provided policy recommendations on AI from a security and privacy perspective.

Interventions by:

- Daniel Loevenich, BSI GISA, Germany
- Bojana Bellamy, President, Center for Information Policy Leadership at Hunton & Williams LLP
- Orestis Trasanidis, EIT Digital | EIT AI Community Lead
- Carolina Rossini, Co-founder, Chief Impact and Partnerships Officer, the DataSphere Initiative, Prof of Law, Boston University

15.30 **Break** (5 min)

15.35 **Topic 2:**
Enabling AI & Data Space Innovation with SMEs in Europe (50 min)
Moderated by Marc Vloemans, Head AI, Cloud Edge (AICE) OpenLab Eclipse Foundation

The second panel discussion will focus on how Europe is working to enable innovative use cases for AI .The focus of this panel will be to elicit insights on how SME innovation and data spaces can accelerate Europe's digital transformation. Eclipse Foundation will show how the AICE open lab will enable Innovation and will lead the discussion with panellists sharing views on enabling AI for SMEs, data spaces, data governance and federated data spaces (e.g. Gaia-X, BVDA).

Interventions by:

- Antonio La Marra, CEO Security Forge, an SME focused on data protection and cybersecurity
- Prof. Fabio Martinelli, Research director of the Italian National Research Council (CNR), Vice Chair, ECSO and expert adviser to H2020 Protection and Security Advisory Group (PASAG)
- Dr. Theo Dimitrakos, R&D Director, Data Sovereignty Huawei and Professor University of Kent
- Thorsten Jelinek, Founder, Digital Platform Governance (DPG) and Director, Taihe Institute, Europe

16.25 **Break** (5min)

Agenda continues on next page

16.30 **Topic 3:**
The Road Ahead, Securing a Global AI Ecosystem & Standards (50 min)
Moderated by Dr. George Sharkov
Vice Chair ETSI SAI, Chief Ass. Professor Plovdiv University & MD Europe Software Institute CEE

The final panel discussion will focus on the latest developments in the standards for AI as well as the drivers for future work on AI security and privacy standards. In addition, this panel will share insights on Data Governance and the challenges of standardization to realize secure international data spaces.

- Ray Walshe, Director EU Standards Observatory, Convener EUOS Foresight Committee, ISO Standards lead, Ireland, GAIA-X Hub National Coordinator, Assistant Professor, Dublin City University
- Prof. Markus Helfert, Director EMPOWER Data Governance National Research Center, Ireland and Director, Innovation Value Institute
- Loretta Tioiela, Co-founder OpenSynBio.org & Fabri-X and member of the European AI Alliance

17:20 **Closing discussion** (30 min)
Moderated by Robin Wauters, Co-founder and editor-in-chief of Tech.eu

- Bojana Bellamy, President, Center for Information Policy Leadership at Hunton & Williams LLP.
- John Suffolk, President, Global Cyber Security & Privacy Officer at Huawei.
- John Higgins (CBE), Chair, Global Digital Foundation.