

Press release

Berlin, June 22, 2021

Privacy-friendly AI for the public sector: Xayn and the Digital Society Institute at ESMT Berlin publish joint position paper

To implement and futureproof governmental AI strategies, we need powerful and GDPR-compliant technology for the public sector. So-called Masked Federated Learning can meet these high requirements for data protection, trustworthiness, and performance. In a position paper published today, the Berlin-based tech company Xayn and the Digital Society Institute (DSI) at ESMT highlight the potential of this decentralized new approach and elaborate on potential use cases in the health sector and law enforcement.

“Countries that want to play a major role in the global AI competition of the future need efficient and, above all, privacy-friendly technologies for the public sector. New decentralized approaches such as masked federated learning combine both – and can thus become an EU model for responsible AI use,” explains Professor Michael Huth, Chief Research Officer at Xayn, Dean at Imperial College London, and co-author of the statement.

“Artificial intelligence also has great application potential in sensitive areas of public services, such as healthcare or public security. Realizing this potential requires privacy-friendly technologies, and they are already available,” emphasizes Martin Schallbruch, Director of the Digital Society Institute at ESMT Berlin and co-author of the statement.

Key points of the joint position paper:

- **Masked Federated Learning** is a form of distributed machine learning that unites data protection and Artificial Intelligence. The raw data always remains on users’ end devices and trains local AI models. These models are aggregated in encrypted form into a global model and fed back. This approach ensures that data protection is maintained, while at the same time efficiently training GDPR-compliant AI.
- The **public health sector** can benefit significantly from the use of federated learning – for example, in preventing and combating future pandemics. For this purpose, cross-device applications (e.g., smartphone apps for assessing personal risk) can be combined with cross-silo applications (e.g., databases of health authorities on the current infection situation). With this collaborative, decentralized technology, individual and collective risks could be assessed more quickly, while at the same time the highly sensitive user data remains on the end devices and is thus always protected.
- For **public safety and law enforcement**, federated learning could be used to support investigations across different police agencies. Police departments could thus benefit from the experiential knowledge of other agencies without sharing personal information with each other. Potential areas of application are cybercrimes, such as identity theft, or offenses involving images of sexual violence against children and adolescents.
- **GDPR-compliant, powerful AI** can increase efficiency, strengthen citizens' trust in the authorities, and become an EU model for the responsible use of AI.

Download: You can download the joint position paper “Artificial Intelligence for the public sector: Masked Federated Learning as a new privacy-protecting solution” [here](#).

About the authors:

[Professor Michael Huth](#) is Co-Founder and Chief Research Officer of Xayn and teaches at Imperial College London. His research focuses on Cybersecurity, Cryptography, as well as security and privacy in Machine Learning.

[Martin Schallbruch](#) is Director of the Digital Society Institute at the ESMT Berlin and teaches at Karlsruher Institute for Technology. He also served as a long-time Director General for Information Technology, Digital Society, and Cyber Security in the German Federal Ministry of the Interior.

[Dr. Leif-Nissen Lundbæk](#) is Co-Founder and CEO of Xayn and specialises in privacy-preserving AI. He studied Mathematics and Software Engineering in Berlin, Heidelberg, and Oxford. He received his Ph.D. at Imperial College London.

[Dr. Clara Herdeanu](#) is Head of Communications at Xayn. She’s handled public relations for tech companies such as Mozilla, Stack Overflow, and Alteryx at the international PR agency Ballou and had also worked for the ebm-papst Group, global market leader in ventilation technology.

[Lola Attenberger](#) is a researcher at the Digital Society Institute at the ESMT Berlin and focuses on cybersecurity. She has studied at the Hochschule für Wirtschaft and Recht in Berlin.

About The Digital Society Institute

The [Digital Society Institute](#) (DSI) is an interdisciplinary research institute of ESMT Berlin, founded in 2015 with the support of leading global companies. It accompanies the economic and social design of digitalization through strategic research and development – with a strong focus on cybersecurity.

About Xayn

[Xayn](#) is a privacy-protecting search engine that enables users to gain back control over the algorithms and provides them with a smooth user-experience. Using the latest AI technology made in Europe, the company ushers in a new generation of user-friendly privacy tech – making privacy available for everyone.

The AI company started as a research project at The University of Oxford and Imperial College London by Leif-Nissen Lundbæk (Ph.D.) and Professor Michael Huth. Together with Felix Hahmann, they founded the tech company in 2017. To this day, that academic vision remains with a workforce comprised of 30% Ph.D.s The company’s open-source framework for federated analytics and learning, XayNet, is the basis of the privacy-protecting personalised search alternative Xayn. The Berlin-based company has received investment funding of 9.5 million EURO by Earlybird VC as well as Dominik Schiener. Xayn has worked with corporations such as Porsche, Daimler, Deutsche Bahn, and Siemens.

About ESMT Berlin

ESMT Berlin is the highest ranked business school in Germany and Top 10 in Europe. Founded by 25 leading global companies, ESMT offers master’s, MBA, and PhD programs, as well as executive education on its campus in Berlin, in locations around the world, online, and in online blended format. Focusing on leadership, innovation, and analytics, its diverse faculty publishes outstanding research in top academic journals. Additionally, the international business school provides an interdisciplinary platform for discourse between politics, business, and academia. ESMT is a non-profit private institution

of higher education, accredited by AACSB, AMBA, EQUIS, and FIBAA, and is committed to diversity, equity, and inclusion across all its activities and communities. [esmt.berlin](https://www.esmt.org)

Press contact

Jennifer Cordes

Public Relations Manager

+49 30 21231-1066

jennifer.cordes@esmt.org