EPIC Insights

AI for security and privacy

Erich Prem
(eutema GmbH)

Yes, that’s right: Artificial intelligence can be your friend when it comes to security and privacy. There is an intensifying debate about AI as a technology enabling privacy intrusion at an unprecedented scale. At the same time, AI-enabled solutions also create new exploit challenges for system security. A third concern is the amount of training data required for AI solutions. In many cases solutions are based on loads of personal data posing even more challenges for people’s privacy.

Much has been said about how we all need to let go of our privacy to harvest the benefits of AI. It has even been argued that Europe’s new and strict data protection rules undermine AI innovation. But there is a new trend emerging: to use AI for improved security and for maintaining people’s privacy.

A range of innovative and often young companies use machine learning or intelligent pattern recognition technologies to detect security threats in computer systems or to help keeping personal data private. As an example, Austrian start-up mostly.ai uses deep learning neural networks to anonymize data. It creates synthetic data models with similar statistical properties than those in the original, non-personal data set. This retains valuable information for most applications that would usually use personal data.

Companies like mostly.ai even benefit from new, strict privacy regulation. Several jurisdictions around the globe are taking inspiration from Europe’s privacy rules thereby also pushing innovation for privacy-preserving technologies. In parallel, increasing concerns about AI security have created new research and innovation challenges for researchers in the AI and security fields. These developments demonstrate how innovation and policy can mutually stimulate each other. Most importantly, it shows that we should not feel victims of technology develoment, but rather take the opportunity to influence their design.

We will discuss these topics at a conference on the role of AI for privacy and security in Singapore on April 9: https://www.epicproject.eu/index.php?id=106. The event is organized by the EPIC project to further EU-Singapore IT cooperation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme (ICT) under grant agreement No 687794.