POLICY BRIEF #5

July 2019

SECURITY, PRIVACY & THE ROLE OF AI: SINGAPORE'S EU COLLABORATION POTENTIAL

EPIC

Europe's ICT innovation partnership with Australia, New Zealand and Singapore

www.epicproject.eu

info@epicproject.eu

@EPIC_ProjectEU

RECOMMENDATIONS

Moving forward, Singapore and the EU should consider the following opportunities for collaboration:

* Improving the dialogue
* Education & training
* Research & innovation empowerment

SUMMARY

Concerns about secure computing systems and personal data protection have risen internationally in parallel to the development of novel AI technology. There are fears that new and powerful AI will be able to break into virtually any IT system, to correlate non-personal data into personal findings, and to generally depend on being fed large amounts of confidential information. On the other hand, there is a massive opportunity in developing AI-related technology to make computer systems safer and keep personal data confidential and under the control of people. The EU with its world-wide recognised data ethics and Singapore with its massive testbed and development of the Smart Nation concept should work together to develop these technologies so that they ensure ethical principles while at the same time maintaining security of systems and utilising the potential power of AI.

INTRODUCTION

Security – from cybersecurity to the Internet of Things – and privacy have become major concerns for citizens, in industry, and also in policy. Artificial intelligence plays an important dual role in this domain: as a source of concern, but also as a source of potential solutions.[1]

Meanings of terms for this brief:[2]

* **Artificial intelligence (AI)**: any decision support mechanism that is strongly data-driven such as those based on decision trees, machine learning, or statistics etc.
* **Privacy**: the ability to exercise control over the processing of one's data and the ability to minimise data that another party learns about you.
* **Security:** refers to ensuring the confidentiality, integrity, and availability, in some contexts it also concerns safety.

It is easy to see how AI, security, and privacy go hand in hand: AI often requires large amounts of training data. In many cases solutions are based on heaps of personal data posing challenges for people's privacy. Secondly, AI itself may enable privacy intrusion at an unprecedented scale through intelligent ways of sifting through and correlating previously uncorrelated data so that it becomes personal. AI-enabled solutions also create new exploit challenges for system security as AI operates an increasing number of networked and internet-connected systems and can also become victim to malicious attacks.

On the other hand, AI can be your friend when it comes to security and 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 keep personal data private. Concerns about AI security have created new research and innovation challenges for researchers in the AI and security fields. This research has benefitted from stricter privacy rules around the world. Europe's data ethics as expressed in its famous General Data Protection (GDPR) and other related laws has become a model for policy makers internationally, and it has also stimulated the demand for new solutions and approaches.

Given the interconnections of today's computing systems and the massive trend towards connected intelligent things and embedded AI, there is a clear need for international collaboration. International forums exist, for example, to discuss cybersecurity (e.g.

[1] Two EPIC events hosted by A*STAR I²R clarified both the industrial and academic research directions and potential, i.e. the EPIC workshop on 'Privacy Preserving Information Technologies'; December 10-11, 2018 and the conference on 'Security and Privacy - The Role of Artificial Intelligence' on April 9, 2019.

[2] Dan Bogdanov, Cybernetica at the EPIC Privacy/AI Event, Singapore, 2019.

at the level of the OECD[3], G7[4]and to a lesser extent the G20[5]). The topic is also discussed in the UN Group of Governmental Experts.[6]

The European Commission has been active in co-ordinating cybersecurity with the member states and with international partners; it has also reach out internationally to explain and further its data ethics and privacy principles. It has created ENISA – the EU Agency for Cybersecurity[7] and addressed important regulation as a part of the Digital Single Market (DSM) initiative. The EU endorses the voluntary non-binding rules of responsible State behaviour by the UN Group of Governmental Experts. Similarly, Singapore follows a strategic approach in cybersecurity and has entered into cooperation partnerships with countries in ASEAN, the US, and Canada, and also with the EU and the UK.[8]

In privacy, the international picture is somewhat less coherent. Depending on the legal system, it is considered a human right (e.g. in the EU), a consumer right or ownership right (as in the US). Also, this is a topic that is still very much emerging, and the international dialogue has really only gained momentum after Europe announced its GDPR and other regulations (DSM). In Singapore, personal data is protected under the Personal Data Protection Act (PDPA). Many companies including large global players followed and decided to adopt a system compatible with European Union laws. This also means that there are huge opportunities for collaboration, innovation opportunities for the industry, and research challenges for academics – from ICT to law, social sciences, and the humanities.

RESEARCH INITIATIVES IN THE EU & SINGAPORE

The Singapore government has been a forerunner in e-government and Smart City technologies. It now also follows a whole-of-government initiative to promote collaboration among agencies, academia, research institutes and the private sector in cybersecurity. A dedicated national cybersecurity R&D programme led by Singapore's National Research Foundation aims to improve the R&D expertise in cybersecurity for Singapore, coordinate and prioritise R&D efforts in cybersecurity across agencies, and create platforms for R&D collaborations among agencies, academia, research institutes and industry. The programme focuses on the development of trustworthy systems, cyber-physical systems security, cyber forensics, and mobile security and cloud security.

A National Cybersecurity R&D Laboratory (NCL) provides computing resources, vulnerable environments, and data sets for repeatable cybersecurity investigation and experimentation environments. The iTrust labs offer a rich set of testbeds for research and businesses to design critical infrastructure.[9]

Singapore has declared privacy a priority for its Smart Nation ambitions: 'Cybersecurity is a key enabler of our Smart Nation. We recognise the possible risks, and prioritise privacy of data and safeguarding of critical systems and networks, even as we make them smart.'[10] Although there have been concerns in Europe about the political system in Singapore, for example about legal limitations potentially reducing freedom of speech,[11] such doubts should not hinder collaboration in science and re-search, especially not as regards privacy-preserving technologies.

The NUS Centre for Research in Privacy Technologies (N-CRiPT) will be based in the National University of Singapore (NUS) School of Computing and affiliated with the NUS Smart Systems Institute. While the primary goal of N-CRiPT is to help prevent privacy leaks, the centre will also look into privacy risk management which includes quantifying the practical risk and potential costs involved in the case of data leakages. N-CRiPT will develop new privacy-preserving solutions for structured and unstructured data, and solutions to protect data throughout its life cycle, from collection and curation to processing and sharing. One technique that N-CRiPT is expected to explore is the generation of synthetic data that mirrors the proportion of the original data sets.

The Strategic Centre for Research in Privacy-Preserving Technologies & Systems (SCRIPTS) will be based in Nanyang Technological University, Singapore (NTU). It will be led by Professor Lam Kwok Yan, Programme Chair (Secure Community) at NTU Graduate College. To translate research into applications, SCRIPTS is expected to provide off-the-shelf solutions to businesses for differential privacy and computing on encrypted data.

Finally, AI Singapore is a national programme in artificial intelligence that was launched in 2017. Its purpose is to catalyse, synergise and boost Singapore's AI capabilities to power its future, digital economy. AI Singapore brings together all Singapore-based universities and research institutions as well as the vibrant ecosystem of AI start-ups and companies developing AI products, to grow the knowledge, create the tools and develop the talent to power Singapore's AI efforts.

In Europe, many research centres now started to investigate privacy preserving technologies including the use of AI. Also, there are several research centres in the EU that closely collaborate with companies in this field including start-ups.[12] Privacy-preserving technology research is already funded in the EU H2020 Framework Programme. This is expected to continue throughout the next Framework Programme 'Horizon Europe'. The European Commission put forward a proposal to network the more than 660 cybersecurity centres in Europe.[13]

[3] http://www.oecd.org/sti/ieconomy/information-security-and-privacy.htm
[4] https://www.banque-france.fr/en/economics/international-relations/international-groups-g20g7/focus-g7-cyber-expert-group
[5] http://www.g20.utoronto.ca/2016/160905-digital.html
[6] https://www.nti.org/learn/treaties-and-regimes/united-nations-groups-governmental-experts/
[7] https://www.enisa.europa.eu/
[8] https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf
[9] https://itrust.sutd.edu.sg/
[10] https://www.smartnation.sg/why-Smart-Nation/transforming-singapore
[11] Having continually improved its position over the last years , SG ranks 66th in the Democracy Index ranking of The Economist's Economic Intelligence Unit. https://infographics.economist.com/2019/DemocracyIndex/
[12] The EPIC Privacy & AI event in Singapore included starts-ups from the EU, from Singapore, and also companies founded by EU expats now based in Singapore.
[13] https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

JOINT ACTIVITIES

The challenges of cybersecurity are global and do not respect national boundaries. Solutions to the problems with which we are faced will need to be developed and implemented in a shared way to reflect this fact. Some collaboration between the European Union and Singapore exists:

* The inaugural **Singapore-UK Joint Grant Call for Cybersecurity Research** was launched in May 2015 and continued with a follow-up call in 2018. The programme focuses on strengthening knowledge and capabilities in cybersecurity, as well as fostering closer collaboration in cybersecurity research between researchers from Singapore and UK.
* **Sopra Steria and A*STAR I²R established a joint R&D laboratory** to collaborate on the development and testing of new cybersecurity technologies for the infocomm technology sector. Sopra Steria, a European leader in digital transformation, provides one of the most comprehensive portfolios of offerings on the market.

Two EPIC events on privacy were able to bring several key European players in this field to Singapore, both from academia and in business. The events initiated a range of collaboration talks followed-up by the planning of research and development actions (e.g. between A*STAR I^{2}R and the French research institutes represented by the IPAL joint lab).

COLLABORATION OPPORTUNITIES

Singapore is ideally located to mediate between the East and the West and has proven to be a place to test new technologies in an environment with a different societal embedding of new IT compared to the EU or the US. The human factor is a key component in both security and privacy and societal and cultural differences can become decisive factors. This includes understanding of cultural aspects such as data ethics, but also the openness to address shortcomings, for example. Thirdly, both security and privacy aspects are usually more densely interwoven with policy and regulation than purely technical systems. This makes international collaboration an imperative.

Therefore, the European Union and Singapore should:

#1 Improve the dialogue

* Intensify the discussion about collaboration in cybersecurity and artificial intelligence
* Perform joint research focusing on ethics of data use
* Jointly showcase technologies combining the benefits of AI with guaranteed privacy and security

#2 Education & training

* Target the education of citizens to better understand the risks, but also solutions in the area of privacy, security and AI. Although data mining, and AI, are game changers and potential threats for personal data protection, there are new exciting possibilities for anonymisation and synthetic data models using machine learning. It is important that more people understand these technologies and how to use them.
* Facilitate an improved exchange between competent players in AI-enabled privacy and security to foster collaboration and dialogue.

#3 Research & innovation

* Demonstrating solutions to inform businesses – including small and medium-sized ones – about the potential for new privacy preserving technology
* Collaborate in privacy-improving and privacy-preserving technologies for Smart City and Smart Nation developments
* Take action to inform key actors in research, technology, and policy about the potential power of ICT to preserve people's privacy while at the same time harvesting the benefits of AI. Inform about the future research and innovation potential in this field, for example through participation in and organisation of conferences and mutual invitations to leading scientists or entrepreneurs.

CONCLUSION

Recent developments in AI, security, and privacy demonstrate how innovation and policy can mutually stimulate each other. Europe's privacy rules have inspired jurisdictions around the globe thereby also pushing innovation for privacy-preserving technologies. Singapore's aim to develop a Smart Nation requires technologies trusted by its people. The EU and Singapore can jointly advance privacy-preserving technologies and secure systems with and for AI technologies. Most importantly, Singapore and the EU can help citizens to not feel victimised by technology development, but rather empowered to influence its design.

ACKNOWLEDGEMENTS

Many experts contributed to this policy brief. The topic of EU-SG AI collaboration was the focus of two dedicated EPIC events in Singapore. Special thanks are due to Tan Chee Seng and Ashok Kumar Marath for their input to this document.

How to cite

When quoting information from this report, please cite the following: „EPIC consortium (2019). *Security, Privacy and the role of AI: Singapore's EU collaboration potential.* EPIC Project policy brief #5."

This policy brief was prepared as part of the EU project EPIC. The views expressed in this brief are solely those of the authors and not of the European Commission or its services.

Europe's ICT innovation partnership with Australia, New Zealand and Singapore

www.epicproject.eu

info@epicproject.eu

@EPIC_ProjectEU

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