Publication: Eurek Alert
Date: 02 March 2020
Headline: Engendering trust in an AI world

Engendering trust in an AI world

SMU Office of Research & Tech Transfer - Can you imagine a world without personalised Spotify playlists, curated social media feeds, or recommended cat videos on the sidebars of YouTube? These modern-day conveniences, which were made possible by artificial intelligence (AI), also present a scary proposition - that the machines could end up knowing more about us than we ourselves do.

According to Gartner's 2019 CIO Agenda survey, 37 percent of Chief Information Officers (CIOs) globally have already deployed AI technology in their organisations. The rapid adoption of AI solutions brings to focus the way data - which could consist of sensitive, confidential and personal information - are being managed and used by organisations.

Speaking at the conference panel on 'AI and Data Protection: New Regulatory Approaches', Singapore Management University (SMU) Associate Professor Warren Chik gave his perspective on how to conceptualise trust in a digital age. "When it comes to matters such as personal data, we don't treat AI as god. Therefore, we cannot rely on faith, which is what religion requires. We need something more substantial than that," he said.

In his talk titled 'Artificial Intelligence and Data Protection in Singapore: Consumers' Trust, Organisational Security and Government Regulation', Professor Chik explained that to engender trust in a digital solution, it is crucial that users are being engaged on the issues involved. "People tend to fear the unknown, and it is hard to have trust in something that you don't know."

Moderated by Professor David Llewelyn, Deputy Dean of the SMU School of Law, the roundtable featured speakers Professor Ian Walden, Centre for Commercial Law Studies, Queen Mary University of London; Associate Professor Yip Man (whose paper was presented by Associate Professor Alvin See on her behalf); as well as commentators Mr KK Lim, Head of Cybersecurity, Privacy and Data Protection, Eversheds Harry Elias; and Mr Lanx Goh, Senior Legal Counsel (Privacy & Cybersecurity) & Global Data Protection Officer, Klook Travel Technology.

AI as an influencer

The ability of an AI system to conduct personal profiling could fundamentally change a user's digital personality, said Professor Chik, highlighting a cause of worry for many.

"While an AI holds specific information such as your name and address, it also forms its own knowledge of your identity, and who you are as a person," Professor Chik said, citing algorithms used by social media feeds to collect data on one's identity, interests and surfing habits. From that data, the system then creates a profile of who they think you are.

"These algorithms - which may be right or wrong - feed you information, articles and links, and as a result brings about an effect on your thinking. In other words, AI can mold human behaviour, and this is a risk that makes a lot of people uncomfortable," Professor Chik said. The threat is very real, he emphasised, noting that regulators have clearly identified a need to regulate the use of data in AI.

In Singapore, for instance, the Protection from Online Falsehoods and Manipulation Act (POFMA) carries criminal provisions on the creation, use and alteration of bots to spread false information.

Publication: Eurek Alert
Date: 02 March 2020
Headline: Engendering trust in an AI world

Data protection legislation: a balancing act

In trying to regulate data, there are always two competing objectives when regulating the use, collection and processing of personal data. "The first objective is to protect the data subject, and the second is to promote innovation," said Professor See, who presented Professor Yip's paper on her behalf.

Of the different types of protection for data subjects that exist today, the most commonly available option is the use of contracts. Professor Yip's paper points out that "[t]he problem with trying to regulate data use through terms and conditions is that in most cases, people don't read [the legal fine print]". The consent given is therefore not genuine.

Professor Llewelyn, who moderated the roundtable, added that the meaning of consent is an issue that needs to be explored in greater depth. "If a consumer were to accept an online contract in full without reading it, can it be realistically said that he or she has agreed to all the terms and conditions, and given full consent?" he asked. "Perhaps there should be legal acknowledgement given to the automatic nature of the commitment made in such contracts."

A more critical limitation of the contract as protection for the data subject, is that the contract only governs the information that is shared between the two parties bound by the contract. For instance, if Facebook were to transfer a user's personal data to a third-party not bound by the contract, the third-party firm will not be obligated to protect the user's information.

Data protection by design

Singapore's Personal Data Protection Act (PDPA), which regulates personal data through the use of legislation, is described as light touch regime that takes a strongly balanced approach between the need for privacy protection and the interest of business innovation.

Professor Yip's paper recognises that there is some level of tension between the two objectives mentioned above. The issue at hand, therefore, is how to strike a balance between individual rights and privacy, and the competing interest of economic growth and innovation, she noted.

At the end of the day, the focus is on preventing, rather than trying to remedy a breach of data privacy. "It is about recognising the rights of the individual and the privacy of their data, and at the same time, the need for organisations to collect, use and disclose personal data for legitimate and reasonable purposes," Professor Yip's paper added.

Another solution that Professor Yip explored in her paper was the use of technology instead of law to protect data subjects. In some cases, privacy can be directly built into the design and operation of operation systems, work processes, network infrastructure and even physical spaces. She nevertheless highlights that this solution is not perfect because it is against the interest of businesses which leverage data to make profits to build robust privacy safeguards into their systems and business models.