ALGORITHMIC TECHNOLOGY: FUELING AI IN AN ETHICAL AND TRANSPARENT WAY

Date: October 20, 2022

Disclaimer: This briefing note contains the encapsulation of views presented by the speaker and does not exclusively represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On October 20, 2022, Dr. Ryan Prox, S/Constable-in-Charge of the Crime Analytics Advisory & Developmental Unit at the Vancouver Police Department and Adjunct Professor at Simon Fraser University, presented on *Algorithmic Technology: Fueling AI in an Ethical & Transparent Way* at the October Digital Roundtable event hosted by the Canadian Association for Security and Intelligence Studies (CASIS)-Vancouver. The key points discussed were algorithmic technology and its implementation within police services; governance, accountability, and public perceptions of AI; and mitigating risk when implementing AI. The presentation was followed by a question-and-answer period with questions from the audience and CASIS-Vancouver executives.

NATURE OF DISCUSSION

Presentation

Dr. Prox discussed the ability of artificial intelligence (AI) to facilitate evidence-based decision-making to probabilistically predict crime, efficiently allocate resources and enhance public safety. Dr. Prox also explored previous failures and current successes of AI through the predictive policing model and discussed risk mitigation and the current legislative framework.

Question & Answer Period

During the question-and-answer period, Dr. Prox discussed trends in the oversight of AI technology within the European Union and Canada, emphasizing the implementation of human review. He also discussed the ethical implications and future implementation of AI in high-risk areas, such as AI used in predicting judicial decisions.

BACKGROUND

Presentation

Dr. Prox stated that predictive policing uses deep-learning trained AI to draw relationships within data to find operationally relevant information and facilitate evidence-based decision-making. Machine learning can either be supervised—humans reviewing the categories of data produced by the trained AI to confirm whether they are correct—or unsupervised—allowing the AI to discern hidden relationships within the data. The method of unsupervised machine learning requires thousands of data features, which falls into the category of 'big data'. Dr. Prox stated that unsupervised machine learning is useful for discerning connections within organized crime and social network analysis.

Continuing on the sophistication and evolution of machine learning, deep learning uses a layered structure of machine learning algorithms called artificial neural networks (ANN). ANN are multi-layers of complex networks of intertwined algorithms that are designed to mimic the neural pathways of the human brain. These systems can learn and train themselves and adjust their neural pathways to obtain better results and even understand its own errors. However, advancements in ANN have historically been hampered by technology limitations, given the massive processing power required and access to millions of data features. Although deep learning was limited to a few key companies five years ago, advancement in GPU (Graphics Processing Unit) technology has expanded the use of deep learning.

According to Dr. Prox, predictive policing effectively provides a probabilistic forecast of whether a property crime will happen or not, and it aims to efficiently allocate police resources to areas with the highest crime, enabling frontline officers with a cutting-edge tool that supplements traditional policing. Typically, forecasts include a number of property crimes (i.e., auto theft, residential, and commercial break and enter). It is worth noting that this technology does not work well with crimes against people, such as violent offences, due to the emotional nature of such crimes that lack a logical decision-making process and motivation to avoid apprehension.

Predictive policing was first implemented in the United States (US) by the Chicago Police Department (CPD) and Los Angeles Police Department (LAPD). The CPD implemented their Strategic Subjects List (SSL) in an attempt to forecast individuals who would likely be involved in future gun-related crimes. However, independent audits found that the system was flawed, and civil liberties groups raised concern that loosely related individuals were suddenly under intense police scrutiny. Further, the LAPD implemented PredPol, but it was found to have used biased data that resulted in police resources being concentrated in marginalized and ethnically diverse neighborhoods. As a result, the American Civil Liberties Union and the Stop LA Spying Coalition initiated legal action, resulting in court ordered consent decrees aimed at reforming police practices and preventing further engagements that deprived individuals of their civil rights and freedoms.

Dr. Prox stated that negative perceptions from US experiences with predictive policing migrated into Canada, despite the community-based policing approach. The two most prevalent issues with the implementation of AI are data bias and algorithmic bias that predispose outcomes. Additionally, AI can produce results that are not explainable (i.e., a black box outcome). The Citizen Lab released an analysis report, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*, on the implementation of predictive policing in Canada, in which many organizations were heavily criticized. However, the Vancouver Police Department (VPD) fared better than most, partially a result of collaboration with international and domestic experts to devise best practices for AI implementation in policing.

The VPD only uses publicly available data in its algorithms, allowing academics and the media to review VPD reporting and outcomes, which helps to enhance transparency and potentially avoid tautological results through outside reporting. Proactive measures by the VPD have included participating in the Regional AI Governance and Industry Code of Conduct Committee; holding a town hall meeting with British Columbia Civil Liberties Association, media, and the general public to address concerns moving forward; engaging with the Citizen Lab for an algorithmic assessment report; and engaging with external auditors for an independent review to examine whether human rights violations are occurring. Dr. Prox stated that these measures that were applied within the VPD were an implementation to reinforce transparency and accountability, which did not happen in the US. Further, a review of the VPD crime forecasting system reported a high confidence level in the results and limited false positives, whereby the model could forecast an incident within a 100-meter buffer, with a 50% to 80% probability. During the evaluation phase of the project, the VPD recorded reductions in residential break and enters between 21% and 29%, before the COVID-19 pandemic.

In terms of emerging policies and regulations to govern the use of AI within the EU marketplace and EU institutions, Dr. Prox noted that the European Union

(EU) has implemented the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act). The AI Act uses a risk-based model to classify whether AI activities are prohibited, high risk, or low risk. Unacceptable risks include social scoring, subliminal or exploitative techniques that cause harm, and remote biometric systems used by law enforcement on the public. Dr. Prox noted that failure to comply with the AI Act can result in fines of up to 10,000,000 Euros and incur personal liability. High-risk implementation includes employee management software, biometric systems used in nonpublic areas, systems to assess creditworthiness, and systems used in the administration of justice. Limited- and minimal-risk systems include AI chatbots, spam filters, and customer- and market-segmentation software.

In Canada, the Directive on Automated Decision-Making (ADM) was implemented on April 1, 2020, setting the minimum requirements for federal use of AI technology. The ADM Directive requires pre-vetting for businesses who have the federal government as a client and requires the source code of AI used in high-risk areas to be approved by a government data scientist.

In addition, the Canadian government is proposing a digital charter, Bill C-27, to balance safety and trust on the use of AI within the private sector; however, the legislation has many factors that have yet to be defined, including the extent to which the legislation will apply intra-provincially. Bill C-27's intent is to ensure AI systems are developed and deployed in a transparent and ethical way that protects the rights of Canadians. The Bill is premised on identifying and mitigating data risk and bias that may impact the public. Thus, responsibility of the AI's algorithm extends to developers on how the technology is implemented by companies and governments by requiring ongoing evaluations and reviews. The Bill requires that businesses have the ability to destroy personal information, vet children's data, and restrict the scope of data collected.

Dr. Prox emphasized that Bill C-27 can hold businesses personally and organizationally liable for data breaches, and it provides remedies against businesses that have violated individuals' privacy, being able to order organizations and service providers to delete personal data. Bill C-27 establishes a new regulatory framework for the development of AI systems under three acts: the Artificial Intelligence and Data Act, Personal Information and Data Protection Tribunal Act, and Consumer Privacy Protection Act. New Criminal Code offenses created by Bill C-27 include failure to create privacy management programs, failure to provide adequate protection of information, failure to obtain consent, unauthorized disclosure, breach of notification, and lack of transparency. According to Dr. Prox, the next piece of legislation will likely be a modified version of Bill C-27 that applies to all levels of government and expands on the ADM Directive. The Bill will likely include more robust enforcement and compliance directives, and enforceable elements may be added to the ADM outside of its ability to acknowledge breaches of the directive.

Question & Answer Period

During the question-and-answer period, Dr. Prox was asked whether he believed the human element should remain behind every final decision-making process, to which he said that within the EU, the AI Act requires that any high-risk activities with a direct impact on individuals must have a human review component. In Bill C-27, there is no language that establishes the context and framework under which human review is mandated and how this oversight is governed. However, the Privacy Commissioner can make orders-in-council that could introduce and reinforce policies aimed at restricting and curtailing high impact systems or implement greater oversight.

In terms of what form of accountability can be expected if AI attempts to "correct" the law to prevent something, Dr. Prox stated that before the implementation of the AI Act in the EU, which heralded in tighter regulations on the use of automated decision-making technology, AI systems were being evaluated, piloted, and tested across a range of scenarios. Some of the most troubling areas of research and development were encroaching into the civil and criminal justice system, including predicting judgements and sentencing outcomes based on an individual's history and involvement in prior offenses. Nevertheless, these activities likely could not continue under the AI Act. Bill C-27 has no hardlines set up that ban the use of AI in certain activities, which leaves it up to the Privacy Commissioner to determine what activities would be prohibited for AI.

KEY POINTS OF DISCUSSION

Presentation

- Machine learning is a subset of Artificial Intelligence, whereby a set of algorithms are fed structured data in order to complete a task. The two most common approaches are supervised and unsupervised machine learning. With supervised machine learning, data is categorized and defined as training data to train the model to recognize patterns or characteristics. Unsupervised machine learning uses data that is uncategorized, and the model looks for common characteristics amongst the data searched, often uncovering hidden relationships within the data.

- Deep learning uses a layered structure of machine learning algorithms called artificial neural networks that mimic the neural pathways of the human brain.
- Predictive policing can effectively forecast property crime patterns, allowing police forces to efficiently allot resources.
- Negative US experiences with predictive policing have come into Canada despite the focus on a community-based policing approach.
- Some of the emerging policies to regulate the use of AI include the GDPR and the AIA in the European Union, and in Canada, the ADM and the proposal of Bill C-27.
- Bill C-27 can hold businesses personally and organizationally liable for data breaches and provide remedies against businesses that have violated individuals' privacy.
- The new Data Protection Tribunal is tasked with reviewing Privacy Commissioner recommendations to impose monetary penalties for contraventions of the Act of up to 5% revenue or $25 million dollars.

Question & Answer Period

- Under Bill C-27, the Privacy Commissioner has the authority to order independent audits, cease action orders, and ordering greater algorithmic transparency, whereby organizations must explain decisions made by a system.
- It is expected that the Privacy Commissioner will more clearly define what activities would be prohibited and under what circumstance algorithmic technology can be applied, while still protecting the rights and privacy of individuals.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/