The Impact of Artificial Intelligence on Data Safety in the 21st Century

Matthew Williams

University of The Bahamas

School of Business

Business Research Methods I BADM-498

Prof. W. Mainga

September 5th, 2023

Identify a broad problem area/topic:

The Impact of Artificial Intelligence on Data Safety in the 21st Century

Research Questions:

- What is Artificial Intelligence?
- Why is data safety important to individuals in the 21st century?
- What are the effects of artificial intelligence on personal consumers as it pertains to data safety?
    - Concentrate mainly on Bahamian consumers while comparing to other nationalities.
- Is artificial intelligence and data safety regulated or planned to be regulated and is it sufficient?
    - What are the policies currently enforced or planned to be implemented, to regulate artificial intelligence and data safety?
        - Compare policies between different countries, while mainly focusing on the Bahamas
    - Are these policies sufficient and address the concerns of the 21st Century personal consumers?
- What strategies can be put in place to regulate Artificial Intelligence and Data Safety?
        - Compare countries strategies while mainly focusing on the Bahamas.

Problem Statement

In the 21st century majority of individuals utilize computing devices such as laptops, tablets, and smartphones to complete their school assignments, work tasks, and operate smart devices around their homes. Due to the amount of work conducted on those devices, companies have to continue to utilize artificial intelligence to allow their services to become more seamless. Artificial intelligence as stated by Fischer and Agnieszka "operates by identifying patterns present in available data and then using this knowledge for new data, the larger the data set the better the possibility for detecting details in relations among data" (Fischer & Piskorz-Ryń, 2021, p. 419). Thus artificial intelligence can collect the consumers' data and utilize it to assist with the advancement of the human race. However, concerns may arise on how are these practices regulated to ensure data safety. Scasssa elaborates that the proposed Artificial Intelligence and Data Act in Canada intends to protect consumers stating "the Minister has the power to order those responsible for AI systems to carry out certain duties or to cease using a high impact system in certain circumstances" (Scassa, 2023, p. 5). This allows the Minister of Innovation, Science and Industry to step in if necessary, similar to the Bahamas. The Bahamas Data Protection Act states "In this Act any restrictions on or exceptions to the disclosure of personal data do not apply if the disclosure is in the opinion of the Minister or the Minister of National Security required for the purpose of safeguarding the security of The Bahamas" (The Bahamas Government, 2003, p. 7). With this in mind concerns may arise such as are these proposed acts enough and does countries like The Bahamas need to revise their Data Protection Act as others seek to revise theirs. Policies and laws which are recognized as key areas elaborated on by Dr. Lilian Mitrou (2018, p. 24). This study will examine the impact of artificial intelligence and strategies that can be implemented to regulate it while protecting personal consumers' data.

Literature Review

Artificial intelligence

Living in the 21st century means you live in a world where the Internet of Everything exists (IoE). The Internet of Everything is recognized as the union of the Internet of Things (IoT) and the Internet of Services (IoS). Ghosh, Chakraborty, and Law cite Cisco stating "the Internet of Everything is the intelligent connection of people, process, data and things" (2018, p. 210). The Internet of Things is the union of Things (devices), Intelligence, and Networks whereas the Internet of Services is the union of Internet Services and Intelligence (Ghosh, Chakraborty, & Law, 2018). This century where the Internet of Everything exists can result in numerous cities like those that lie within The United States of America, China, and The Bahamas being seen as smart cities.

Smart cities are cities that connect numerous devices together throughout the city to offer "enhanced social facilities, transport, and accessibility while promoting sustainability by using different sensors to gather data from the surroundings" (Ahmed, et al., 2021). These smart cities include infrastructure used by the medical field which "are necessary to access, analyze and rapidly manage cross-scale big data in biomedical research and enhance the use of artificial intelligence" (Zhu & Zheng, 2018, p. 1). Upon this data being collected from the Internet of Things (IoT), Artificial Intelligence (AI) uses the data, by analyzing, processing, and outputting data to make the lives of humans easier. "IoT needs to depend on AI as it is impossible for any human to find information in the data that IoT generates" as stated by Ghosh, Chakraborty, and Law (2018, p. 212). Ghosh, Chakraborty, and Law further expand, elaborating that AI is also capable of detecting patterns within the big dataset generated by smart cities which is recognized

as Big Data, which is not possible for a system that does not have AI involved. Supporting these claims Mitrou states that “AI can cope with the analysis of big data in its varying shapes, sizes and forms” (2018, p. 17). Thus Artificial Intelligence may be recognized as the intelligence involved in a system or network. As stated by Mitrou it is an “intelligent machine which … perceives its environment and takes action that maximize its chances of success” (Mitrou, 2018). Similar to human intelligence, AI is able to learn. It learns through an approach recognized as machine learning which allows it to process data and analyze the patterns within the data to generate new data, thus the reason why it can be recognized as the intelligence involved within smart cities.

Smart cities becoming more popular as a “worldwide study, which surveyed over 4500 policy-makers across various industries, 45% of big enterprises, and 29% of small and medium-sized enterprises reported AI use” as stated by Ishaq Mohammed confirms this (2020, p. 172). This is caused by the positive effects of AI which Minzhen Xie elaborates on, one being it “can automate ‘programmable work’ ” resulting in lower costs for labor (2019, p. 4). Other researchers agree that these smart cities have positive effects stating “smart cities can enable population-wide surveillance, counteract ageing … and provide quick and effective responses to emergencies and disasters such as outbreaks” (Bragazzi, et al., 2020, p. 6). Many of the impacts though general trickle down to personal consumers as they utilize the services that smart cities offer daily and are heavily affected by the responsiveness to disasters and outbreaks. Thus when this growth of smart cities is observed more concerns about individuals’ personal data arise.

Data Safety

Data is generated in large sets by smart cities which then await to be used by AI. AI can read this data and learn from it consequently concerns arise from this as many value their privacy. As stated by Mitrou "personal data and artificial intelligence are 'a two-way street': personal data feeds AI and IA produces inferred data" (2018, p. 19). The personal data that Mitrou speaks about is often times granted to the AI by the user via their consent. This personal data can include but is not limited to banking information, residential address, email address, passport information, driver's license information, passwords, and many other forms of personal information that are a part of the big dataset. This can become a concern for personal consumers as when their information is provided to different things (devices) or services that reside in the network of IoE, a possible data breach can occur resulting in a breach of their personal data. A data breach that releases individuals' personal data can result in numerous outcomes from financial fraud to their social media accounts being hacked. For example, Ahmed et al. mention a data breach that leaked "roughly 50 million Facebook profile data" (2021, p. 43). Some may also be concerned about how AI is using their data for the processes which it carries out, consequently practices and laws and been implemented to address some of these issues. These issues can affect individuals across the globe and are not limited to a single country.

Some countries have more devices and depend more on the IoE which includes the healthcare, financial, education, and other systems of countries. The Bahamas in comparison to other countries like China and the United States of America is not as technologically advanced. Thus, a data breach within certain systems of The Bahamas would have a different impact. As elaborated on by Wang, Zhang Lassi, and Zhang this was the way that most countries stored records in the past but "nowadays, patient information is increasingly recorded digitally and

electronically" (2022, p. 1). The Bahamas to date still uses physical records alongside electronic ones at Princess Margaret Hospital (PMH) thus a data breach within the hospital in The Bahamas would not have the same impact as another country where records are only stored electronically. In the event, that PMH is breached medical staff can turn to the physical records to still allow them to save lives. However, as the archipelago becomes more cashless and ventures into cryptocurrency, recognized as the Sand Dollar, a breach in the financial sector can become a major concern.

Mohammed's article elaborates on how AI can make data more secure (increase data safety) as due to its learning patterns it can "detect [inappropriate actions] and take appropriate action, such as notifying a technician or returning to a safe position after a malware" (2020, p. 174). Malware and viruses are sometimes utilized to attack things (devices) within the IoE, resulting in the comprise of those devices which can lead to a data breach, or the data being destroyed. So while AI does have a negative effect on data safety due to its demand for a large database it also protects against cyber-attacks which aim to use that data for wrongdoing. However as argued by Mohammed "AI systems are taught using data sets, you will need to collect a large number of different sets of malware codes, non-malicious codes, and anomalies to train your system" (2020, p. 175). Thus, acquiring this data can become time-consuming and an issue for ensuring protection consequently lawmakers have established laws to assist with these issues.

Legislation

Policy and Lawmakers have often tended to create policies to mitigate problems that affect their jurisdictions, they also create such laws and policies to protect their citizens,

residents, and members of their jurisdictions. Gregory, Henfridsson, Kaganer, and Kyriakou mention that a mechanism that will make AI more "likely to perceive sustainable value" by consumers includes "respect to platform legitimation" (2021, p. 547). The authors further elaborate on the meaning of platform legitimation meaning that "principles of privacy", "security by design", "and by ensuring the explainability of predictions generated by AI on the platform" are implemented to ensure users' personal data is collected responsibly (Gregory, Henfridsson, Kaganer, & Kyriakou, 2021, p. 547). Due to concerns that arose with data safety numerous countries including The Bahamas, the United States of America, China, and other countries.

European Union

The European Union has continuously proven itself to remain up to date with its legislation as it pertains to technology. "The birth of data protection in Europe, especially the Data Protection Directive 95/46/EC was linked to the impressive developments of the 70s" as mentioned by Mitrou shows the union's dedication to the topic of technology (2018, p. 24). The European Union also has the General Data Protection Regulation (GDPR) which was established in 2018. The Union also as stated by the author provides their citizens and residents with rights, one being "the right to privacy and the protection of personal data [which] are fundamental and binding rights" (Wang, Zhang, Lassi, & Zhang, 2022, p. 14). The European Union also doesn't allow countries that do not have protection that is up to their standard to have data transfers with them. Based on the articles mentioned in this study the European Union legislation is adequate as it pertains to AI and data safety, unlike counterparts like China.

China

China's legislation which mainly impacts AI as stated by Wang et al. is the Personal Information Protection Law (PIPL), Cybersecurity Law, and the Civil Code alongside national

standards. These legislations include “specific rules pertaining to individual consent and authorization for data processing, wherein subjects receive, at a minimum, the purpose for the information processing, along with its manner and scope” (2022, p. 2). Unfortunately, these regulations and laws do not speak to how big data is processed or used. Wang et al. believe that the legislation which is established in China can be strengthened as it. Khisamova et al. support that China’s legislation is not equal to the United States of America’s or the European Union’s stating that though China has numerous “breakthrough[s] in the development of artificial intelligence” the country's legislation only focuses on ‘the economic benefits of introducing artificial intelligence” (2019, p. 5161). However, Cowls et al. mention that in 2017 released its strategy for developing AI known as “New Generation Artificial Intelligence Development Plan” this plan aims to increase the amount of ways AI is used. Cowls et al. further mention that Robin Li stated before that Chinese individuals are not concerned about privacy issues. This eventually leads to the article further mentioning that China has an issue with privacy legislation due to the “weakness of [its] … judicial system (Cowls, et al., 2020). These articles elaborate on the grey area that exists as it pertains to data privacy in China, however, based on Cowls et al. these grey areas may not be an issue for the Chinese people. Whereas in the United States of America, one’s privacy is valued much more.

The United States of America

The United States of America has numerous Acts that speak to AI and data protection which is more mature when compared to China or The Bahamas. China’s legislation as elaborated on by Wang et al. tends to be broad which is not the same as The United States of America whose legislation is more specific (2022). These Acts include but are not limited to the “Health Insurance Portability and Accountability Act of 1996(HIPAA)”, “the Standards for

Privacy of Individually Identifiable Health Information of 2000", and "the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009" as stated by Wang et al. (2022, p. 7). The acts previously mentioned mainly affect AI and data safety as they pertain to the medical field and personal data in that industry. The country also has a National Strategic Research and Development Plan for Artificial Intelligence which is recognized as a development and research plan funded for AI as stated by Khisamova et al. (2019, p. 5161). The United States of America as elaborated on by Wang et al. though concerned about the privacy of their residents and citizens' data they are more liberal in comparison to the European Union. The country has legally binding provisions that allow data to flow between countries as they form trade agreements with countries agreements "such as USMA and the U.S. Japan Digital Trade Agreement" (2022, p. 14). The United States of America is more invested in AI than The Bahamas but the consumers in The Bahamas do follow the trends of their northern neighbors.

The Bahamas

The Bahamas has numerous laws that speak to data safety however there is no legislation that speaks directly to AI The Computer Misuse Act states "any person who, without authority, knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in any computer shall be guilty of an offence" (The Bahamas Government, 2006, p. 6). Thus, Act however can be interpreted to include the parameters of AI. Mutual Legal Assistance Act, Computer Misuse Act, Electronic Communications and Transactions Act, Criminal Procedure Code Act, Data Protection (Privacy of Personal Information) Act, and the Sexual Offences and Domestic Violence Act are parts of legislation that affect either AI or data safety. However, due to the lack of updated amendments made for these Acts, they can become outdated quickly as the technology behind AI upgrades. The Bahamas also appears to have

legislation that is broad similar to China's legislation however due to the lack of research material on The Bahamas as it pertains to AI a literature gap lies in that topic. Unlike the other countries, The Bahamas has not publicly made an announcement of plans for AI and its direct impact. The Bahamas Data Protection Act however, speaks to the protection of "personal data" however it does not specify the results of breaches of personal data that sits in big datasets which AI uses to work efficiently and learn (The Bahamas Government, 2006, p. 7). Additionally, It appears as though research has not been conducted in the country to understand if their concerns with data safety and AI are currently being addressed by these laws.

Generalization in legislation as it pertains to AI and data safety can present issues especially as the use of AI becomes more dominant in the country.

Recommendations

"While the potential for richer data and therefore richer insights is enormous … careful consideration of consent privacy and other ethical issues will be of paramount importance" are the words of Andrew Bate and Steve Hobbiger (2020, p. 130). A large portion of the literature pertaining to computing technology speaks about individuals' needs for privacy thus when considering recommendations for AI and data safety the recommendation of keeping individuals' personal data secure is paramount. Miriam Buiten recommends that legislation propose to have "transparency requirements for AI" (2019, p. 45). Buiten article later elaborates on how transparency requirements can allow lawmakers to hold AI creators accountable for decisions made by the intelligence and it will also allow the victim to be made aware that the algorithm can cause a potential breach. Khisamova et al. recommendation is that the legal responsibility should have different levels as it pertains to users and developers of AI (2019, p. 5161). AI can also be implemented as expanded on by Mohammed et al. to be used as cybersecurity to prevent data

breaches, preventing individuals' personal data from entering the hands of individuals who can use it for wrongdoing (2020). These recommendations can prove to be beneficial to countries like China and The Bahamas, however, due to the lack of research it can become difficult to select the recommendation which may work best for the archipelagic nation.

References

Ahmed, S., Hossain, M., Kaiser, M., Noor, M. B., Mahmud, M., & Chakraborty, C. (2021, April 29). Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities. *Data-Driven Mining, Learning and Analytics for Secured Smart Cities*, 23-47. doi:10.1007/978-3-030-72139-8_2

Bate, A., & Hobbiger, S. F. (2020, October 7). Drug Safety. *Artificial Intelligence, Real-World Automation and the Safety of Medicines, 44,* Springer Nature Switzerland. doi:10.1007/s40264-020-01001-7

Bragazzi, N. L., Dai, H., Damiani, G., Behzadifar, M., Martini, M., & Wu, J. (2020, May 2). How Big Data and Artificial Intelligence Can Help Better Manage the COVID-19 Pandemic. *International Journal of Environmental Research and Public Health, 17*(9), 3176. doi:10.3390/ijerph17093176

Buiten, M. C. (2019). Towards Intelligent Regulation of Artificial Intelligence. *European Journal of Risk Regulation, 10*(1), 41-59. doi:10.1017/err.2019.8

Cowls, J., Morley, J., Taddeo, M., Wang, V., Floridi, L., & Roberts, H. (2020, June 17). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Society, 35*, 59-77. doi:10.1007/s00146-020-00992-2

Fischer, B., & Piskorz-Ryń, A. (2021, January 1). Artificial intelligence in the context of data governance. *International Review of Law, Computers & Technology*, 419-428. Retrieved September 1st, 2023, from https://eds-p-ebscohost-com.cob.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=5&sid=568ae276-c880-4efe-9711-145405569809%40redis

Ghosh, A., Chakraborty, D., & Law, A. (2018, November 14). Artificial intelligence in Internet of things. *CAAI Transactions on Intelligence Technology*, *3*(4), 208-218. doi:10.1049/trit.2018.1008

Gregory, R. W., Henfridsson, O., Kaganer, E., & Kyriakou, H. (2021, July 15). The Role of Artificial Intelligence and Data Network Effects for Creating User Value. *Academy of Management Review, 46*(3). doi:10.5465/amr.2019.0178

Khisamova, Z. I., Begishev, I. R., & Gaifutdinov, R. R. (2019, November). On Methods to Legal Regulation of Artificial Intelligence in the World. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 5159-5162. doi:10.35940/ijitee.A9220.119119

Mitrou, D. (2018, December 31). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? *SSRN Electronic Journal*, 1-90. Retrieved Septemeber 19, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914

Mohammed, I. A. (2020, September). Artificial Intelligence for Cybersecurity: A systematic mapping of literature. *INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT] , 7*(9). Retrieved September 19, 2023, from https://www.researchgate.net/publication/353887583_ARTIFICIAL_INTELLIGENCE_FOR_CYBERSECURITY_A_SYSTEMATIC_MAPPING_OF_LITERATURE

Scassa, T. (2023, May 25). Regulating AI in Canada: A critical look at the Proposed Artificial Intelligence and Data Act. *The Canadian Bar Review*, 1-30. Retrieved September 1, 2023, from https://eds-p-ebscohost-

com.cob.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=5&sid=568ae276-c880-4efe-9711-145405569809%40redis

The Bahamas Government. (2003). Data Protection. The Bahamas. Retrieved from http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf

The Bahamas Government. (2006). Computer Misuse Act. *The Bahamas Consitution*, pp. 1-15. Retrieved from http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf

Wang, C., Zhang, J., Lassi, N., & Zhang, X. (2022, September 27). Privacy Protection in Using Artificial Intelligence for Healthcare: Chinese Regulation in Comparative Perspective. *Healthcare 2022, 10*(10), 1878. doi:10.3390/healthcare10101878

Xie, M. (2019). Development of Artificial Intelligence and Effects on Financial System. *Journal of Physics: Conference Series, 1187*(3), 1187. doi:10.1088/1742-6596/1187/3/032084

Zhu, L., & Zheng, W. (2018, Septemeber 18). Informatics, Data Science, and Artificial Intelligence. *Journal of the American Medical Association, 320*(11). doi:doi:10.1001/jama.2018.8211