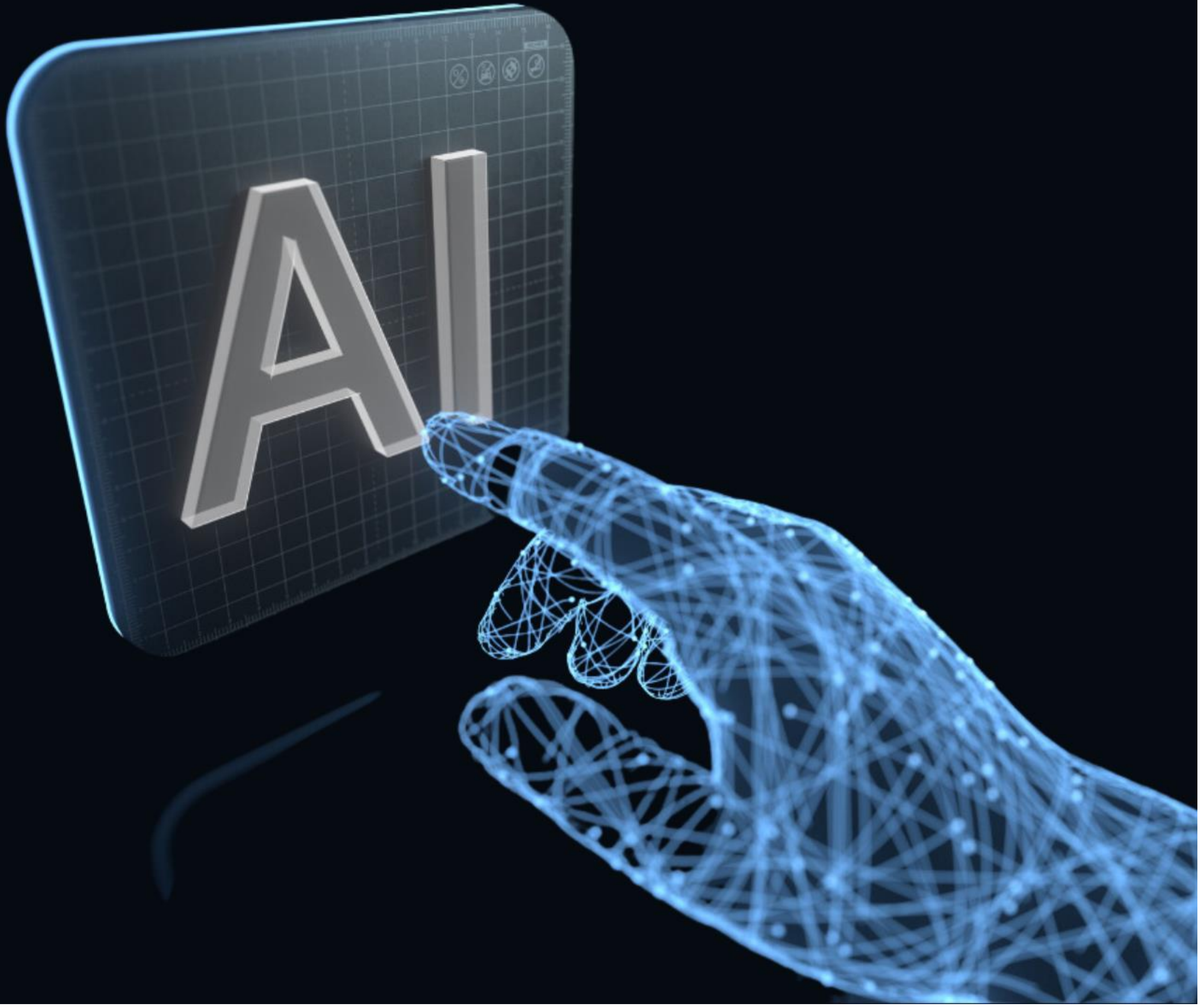
Legal Considerations for a Safe and Responsible AI Future in Australia

Submission by:

Brenda van Rensburg (Terrene Global)
2023



Contents

I. Executive Summary

The integration of Artificial Intelligence (AI) into our society marks a significant milestone in humanity's progress. According to Steven Pinker, progress is made by 'making changes in social institutions like laws and educational systems.' The development and subsequent interaction with AI have unveiled a range of legal issues that must be addressed sooner rather than later. This comprehensive analysis explores the interplay of key aspects in the realm of AI, including data quality and responsible usage, algorithms and law, privacy and security, and criminal and civil procedural challenges.

To effectively tackle these complex topics, it is imperative that we engage in meaningful discussions and propose practical and legal solutions through thoughtful dialogue between regulators, creators, and users. This entails carefully examining the specific challenges and potential risks associated with AI, and developing comprehensive frameworks that ensure responsible and ethical AI practices.

By addressing these various considerations, we can pave the way for a legal AI landscape that maximizes its potential while safeguarding our Australian society. Through collaborative efforts and thoughtful deliberations, we can establish a solid foundation that balances innovation with the protection of our citizens' rights and well-being.

II. Introduction

The trajectory of technological advancement has undergone an extraordinary surge, as evidenced by the integration and extensive utilization of AI, surpassing all preceding rates of growth. Accompanying this progress is an undeniable upsurge in global and domestic discussions surrounding the implications and applications of AI.

Australia has recently taken a significant step by fostering an inclusive dialogue, inviting its residents to actively participate in shaping the future of "Safe and Responsible AI in Australia". Given the pervasive deployment and information gathering through A.I. in our communities, it becomes crucial for the government to carefully evaluate potential legislative gaps that will impact the balance between innovation and the protection of our citizens' rights and well-being.

Recently notable efforts have been observed from the European Union, the United States, and Canada as they actively engaged in substantial discussions centered around AI.[1] The outcome of these discussions has materialized in the form of concrete AI strategies and ethical guidelines.

'The Australian Government's vision is to implement world class data and digital capabilities to deliver outstanding outcomes for all.'[2] Undoubtedly, the pursuit of data and digital excellence can be greatly accelerated by harnessing the transformative power of AI. However, as Australia progresses towards becoming a 'data-informed and digitally capable' nation, it is imperative to approach the integration of AI with a thoughtful and cautious mindset.

By establishing comprehensive legal frameworks, we can foster the responsible advancement of AI while also ensuring that individuals have appropriate channels for seeking legal remedies in case of

[1] BLG, Emerging technologies series: Regulating artificial intelligence in Canada, the U.S. and Europe (Vlog, 2023) <https://www.blg.com/en/insights/2023/05/regulating-artificial-intelligence-in-canada-the-us-europe>.
[2] Australia Government, Data and Digital Government Strategy: The Data and Digital Vision for a World-Leading APS to 2030 (2023)

any harm. This approach aims to strike a harmonious equilibrium, allowing for the progress of AI technology while safeguarding the rights and welfare of the Australian population.

This submission will underscore the critical importance of legal considerations in the development of AI across several key areas, namely:

- Data Quality & Ethical Usage
- Algorithms and Law
- Privacy & Security
- Criminal & Civil Procedural Challenges

These topics will be explored to shed light on their significance and provide insights into the necessary measures that should be taken to address them effectively. The implementation of legislation and legal frameworks for A.I. becomes a driving force for societal advancement while prioritizing the protection of citizens' rights, privacy, and overall well-being.

III. Data Quality, Ethical Data Usage, and Legal Implications in AI Systems

Improving data quality and promoting responsible data usage are paramount in the field of AI. Data quality encompasses the reliability, accuracy, and usability of the data utilized in AI systems[3], while responsible data usage involves ethical and transparent utilization of data inputs.[4] By striking a harmonious balance between data quality and responsible data usage, we can cultivate AI systems that are trustworthy, safeguard privacy, and uphold ethical practices.

Data quality assumes a pivotal role in the effectiveness and performance of AI systems. It is imperative to ensure that data inputs are reliable and suitable for their intended purpose, as this is crucial for accurate learning, pattern recognition, and decision-making processes.[5] High-quality and dependable data strengthens the robustness of AI algorithms, enabling them to derive meaningful insights, make precise predictions, and generate reliable outputs. Consequently, addressing concerns related to data quality is of utmost importance when constructing dependable AI systems.

Responsible data usage is equally important in the ethical and transparent operation of AI systems. It involves the proper handling, utilization, and governance of data to mitigate risks, protect privacy, and uphold ethical principles. Responsible data usage considers factors such as consent, data anonymization, and adherence to privacy regulations to safeguard individuals' rights and prevent misuse or unauthorized access to personal information.[6] By prioritizing responsible data usage, we can build trust with users and stakeholders, ensuring the ethical utilization of data in AI applications.

While the following discussion will explore data quality and data usage as separate aspects, it is important to recognize that they share similarities, especially within the context of AI. The intertwining of data quality and responsible data usage requires a holistic approach to data management in AI. Data quality initiatives focus on assessing and improving the reliability, accuracy, and usability of data inputs, ensuring they meet established standards. Simultaneously, responsible data usage practices emphasize the ethical collection, storage, and utilization of data to maintain privacy, protect sensitive information, and respect individuals' rights. By integrating both aspects, AI systems can operate with a higher level of integrity, promoting transparency and accountability.

(a) Data Quality

Data quality encompasses several important factors, including reliability, accuracy, consistency, completeness, and suitability.[7] It refers to the overall fitness for purpose and appropriateness of data for its intended use. When data exhibits high quality, it is devoid of errors, inconsistencies, and discrepancies, accurately reflecting the real-world entities or phenomena it seeks to capture.[8] Key elements of data quality encompass data accuracy, completeness, consistency, timeliness, and

[3] Anand Deshpande and Manish Kumar, *Artificial Intelligence for Big Data* (Packt, 2018).

[4] Christine Cepelak, An Introduction to Data Ethics: What is the Ethical Use of Data? (blog page) < https://www.datacamp.com/blog/introduction-to-data-ethics>.

[5] Anand Deshpande and Manish Kumar, *Artificial Intelligence for Big Data* (Packt, 2018).

[6] V. Naresh Kumar and Prashant Shindgikar, *Modern Big Data Processing with Hadloop* (Packt, 2018).

[7] Editor Neera Bhansali, *Data Governance: Creating Value from Information Assets* (CRC Press, 2013).

[8] Alessandro Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (Asser Press, 2022).

validity.[9] The assurance of data quality is essential to enable effective decision-making, analysis, and the production of reliable outcomes in diverse domains such as business, research, and governance.

In an AI-driven world, the impact of data quality issues becomes even more pronounced, as they can have significant repercussions on outcomes and decision-making processes. These issues encompass a range of challenges, including inaccuracies, incompleteness, inconsistencies, duplicates, outdatedness, non-standardization, and data bias. When these data quality issues persist within AI systems, they can amplify the risks and result in significantly adverse outcomes.

Over the decades, data collection has undergone significant transformation. Initially, data was primarily gathered to cater to customer needs, gain insights into customer behaviour, and enhance marketing strategies. However, with the evolution of technology, the importance of data quality has become paramount. It is now widely recognized that inadequate data quality can have far-reaching consequences. From the unauthorized disclosure of personal and sensitive information to wrongful arrests, compromised navigation systems, and potential impacts on critical infrastructure like water and energy, the implications of poor data quality are profound. Ensuring high-quality data has become essential in safeguarding individuals' rights, maintaining public safety, and upholding the integrity of our increasingly data-driven society.

The wrongful arrest and imprisonment of Randall Reid in November 2022 brought attention to critical data quality issues and their potential impact on privacy in the context of AI technologies.[10] Initially, the Jefferson Parish Sheriff's Office utilized AI facial recognition technology to link Reid to a series of thefts, leading to his unjust incarceration for a week. However, Reid consistently asserted his innocence, emphasizing mistaken identity as the root cause of the misidentification.[11] It was only when his attorney, Tommy Calogero, intervened and presented compelling evidence revealing significant disparities between Reid and the actual perpetrator that the warrant was ultimately revoked.

This case serves as a poignant example of the risks associated with the evolving nature of data collection and its intended use. Over time, the purpose and intent behind data collection can change, leading to potential privacy infringements. The data collected, particularly when it includes personally identifiable information, may be utilized beyond its original intended scope, raising concerns about privacy violations.

The case of Randall Reid highlights the need for strong data quality standards and responsible data practices in the context of AI technologies. It underscores the importance of recognizing and addressing errors, biases, and unintended consequences that can arise from the use of data in AI systems. By prioritizing data quality and adhering to robust privacy safeguards, we can mitigate the risks of privacy infringements and ensure that data is used in a manner that respects individuals' rights and maintains their trust in the technology.

[9] Editor Neera Bhansali, *Data Governance: Creating Value from Information Assets* (CRC Press, 2013).

[10] NBC News, Facial Recognizion Tool Led to Mistaken Arrest, Lawyer Says (web page, 2023) <https://www.nbcnews.com/tech/security/facial-recognition-tool-led-mistaken-arrest-lawyer-says-rcna64270>.

[11] Kashmir Hill and Ryan Mac, Thousands of Dollars for Something I Didn’t Do (Web Page, 2023)< https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html>.

(b) Data Usage

Predictive analytics provides a compelling illustration of the utilization of data, allowing us to anticipate future events and trends.[12] However, it is essential to consider the legal implications, particularly regarding the potential exploitation of personal data. Target's controversial use of customer data in 2012 serves as a notable case in point. By analysing purchasing patterns and demographic information, Target developed a sophisticated algorithm capable of accurately predicting pregnancies.[13] The intent was to target expectant mothers with personalized marketing campaigns. Nevertheless, this raised ethical concerns when a teenage girl's pregnancy was identified by Target before her family was aware, leading to debates on privacy rights and responsible data use.

Another instance involving the New York Police Department (NYPD) and Azavea, a technology company, occurred in 2015.[14] They implemented a predictive policing system, named 'Patternizer,' which employed AI and historical crime data to forecast and prevent crime.[15] However, an audit[16] revealed biases in the system's outputs due to insufficient historical data and the presence of "dirty data"—missing, incorrect, or non-standardized information.[17] These findings, combined with incidents of police brutality, such as the Floyd case, resulted in lawsuits and concerns regarding the reliability of historical data. The unethical application of predictive policing, exemplified by the flawed system used by the NYPD, contributed to disproportionate convictions among individuals from lower socio-economic backgrounds, perpetuating social inequalities and compromising fair judicial trials.

These examples highlight the legal considerations associated with data-driven practices, particularly in the domains of targeted advertising and predictive policing. They raise questions about privacy rights, data collection, and the responsible use of personal information by companies and law enforcement agencies. Clear guidelines and regulations are needed to ensure individuals' privacy protection and mitigate the potential biases and flawed outcomes that can arise from data utilization in the age of AI and big data.

[12] Daniel Vaughan*, Analytical Skills for AI & Data Science: Building Skills for an AI-Drive Enterprise* (O'Reilly, 2020).

[13] Kashmir Hill, How Targer Figured Out a Teen Girl was pregnant before her Father did (web page, 2012) <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=1786a1c16668>.

[14] Laura Nahmias and Miranda Neubauer, NYPD Testing Crime-Forecast Software (web Page) < https://www.politico.com/states/new-york/city-hall/story/2015/07/nypd-testing-crime-forecast-software-090820>.

[15] Andrew Liptak, The NYPD is Using a New Pattern Recognition System to Help Solve Crimes (web page, 2019) <https://www.theverge.com/2019/3/10/18259060/new-york-city-police-department-patternizer-data-analysis-crime>.

[16] J. Brian Charles, NYPD's Big Artificial-Intelligence Reveal (web page, 2019) < https://www.governing.com/archive/gov-new-york-police-nypd-data-artificial-intelligence-patternizr.html>.

[17] Won Kim et al., A Taxonomy of Dirty Data (2003) 7 *Data Mining & Knowledge Discovery* 81.

IV. Algorithms, and the Legal Landscape in the Age of AI

Data and algorithms are interconnected and rely on each other in the context of AI and machine learning. Algorithms are designed to process and analyze data, extracting meaningful insights and patterns. On the other hand, data provides the input for algorithms, serving as the fuel for training models and making predictions or decisions. Without data, algorithms would have nothing to operate on, and without algorithms, data would remain raw and unprocessed. Therefore, the combination of data and algorithms is essential for the functioning of AI systems.

Various types of algorithms are utilized to fulfill different purposes within the realm of AI. Commonly employed AI algorithms encompass a range of techniques, including supervised learning, unsupervised learning, reinforcement learning, deep learning, natural language processing, and genetic algorithms.[18] These algorithms are designed to process data and extract meaningful insights based on their specific objectives. However, it is essential to recognize that the use of data in AI applications can raise concerns, particularly when it comes to personal and sensitive data. The potential for multiple and unintended uses of data underscores the importance of responsible data practices and safeguarding individuals' privacy.

AI systems have demonstrated the ability to learn from past actions and corresponding responses. Machine learning algorithms and big data-powered systems enable AI to perform complex tasks such as autonomous driving, medical data analysis, and executing intricate financial transactions.

While government agencies and organizations have witnessed successful outcomes through the implementation of algorithmic technologies, they have also encountered significant challenges and negative repercussions, as demonstrated by the notorious Robodebt scheme. The detrimental impact of flawed algorithmic decision-making came to light with the Robodebt scheme between 2016 and 2019, which resulted in over half a million inaccurate Centrelink debts being raised. Tragically, this caused significant harm, with some individuals committing suicide.[19] The increasing reliance on algorithmic decision-making by governments to deliver public services, as highlighted by Tapani Rinta-Kahila, raises concerns when human involvement is removed from the equation. [20] In 2020, the government eventually acknowledged that 470,000 debts had been falsely raised, leading to a catastrophic outcome that drew widespread media attention to the Australian government. [21] As Robodebt was an autonomous algorithmic system, it can be argued that it falls within the realm of AI, thus highlighting the legal issues that can result from errors or inaccuracies within AI systems. The case of Robodebt serves as a distressing example of the potential consequences and societal impact when relying on autonomous AI systems for decision-making in sensitive areas.

[18] Andres Rodriguez, *Deep Learning Systems: Algorithms, Compilers, and Processors for Large-Scale Production* (Margan & Claypool, 2020).

[19] Courtney Gould, Mother of Son who Dide by Suicide after Robodebt Share Tragic details on Find in his Home (web page) <https://www.news.com.au/lifestyle/health/mental-health/mother-of-son-who-died-by-suicide-after-robodebt-shares-tragic-detail-on-find-in-his-home/news-story/ee5016ac58b83c8c1560eaacfaba10bb>.

[20] Tapani Rinta-Kahila, Algorithmic Decision-Making and System Destructiveness: A Case of Automatic Debt Recovery (2020) 31 *European Journal of Information Systems* 3.

[21] Noel Cressie, Robodebt Not Only Broke the Laws Of The Land – It Also Broke Laws of Mathematics (web page, 2023) <https://www.uow.edu.au/media/2023/robodebt-not-only-broke-the-laws-of-the-land--it-also-broke-laws-ofmathematics.php>.

In 2014, an Amazon AI-powered recruiting system was developed. It was later revealed that the training data predominantly consisted of male candidates. [22] This resulted in biased outcomes as the AI, influenced by the skewed data and its learning capabilities, learned to differentiate between male and female resumes based on the specific choice of words used. [23] Consequently, the system exhibited a preference for men, disadvantaging female candidates in the recruitment process.

High-frequency trading employs algorithmic equations within the international financial markets.[24] In 2010, algorithms were identified as the catalyst for the flash crash of the British Pound, resulting in a staggering global financial loss exceeding $2 trillion.[25] Citibank acknowledged responsibility for the incident, as their London branch mistakenly input repeated sell orders that exacerbated the plummeting value of the pound. The UK Financial Conduct Authority (FCA) imposed a fine of £17.9 million on Citigroup.[26] However, as of the current compilation of this submission, there is no available evidence to substantiate the claim that individuals affected by this event were never compensated for their significant losses.

All of these examples emphasize the increasing concerns surrounding the appropriate utilization of data and algorithms, particularly in contexts where human involvement is limited. To address these concerns, it is crucial to adhere to the principles outlined in the AI Bill of Rights.[27] This includes conducting independent evaluations and providing transparent, accessible reports through algorithmic impact assessments. These assessments should encompass comprehensive testing to identify and address any disparities, while also implementing effective mitigation strategies.

The onus of proof in a civil proceeding rest on the plaintiff, but when an individual faces the overwhelming power of a government or global entity like Amazon, Facebook or Google, the balance of power becomes skewed and unjust. This imbalance creates significant hurdles for individuals in asserting their rights and providing evidence of discrimination or unfair debt practices. The immense authority wielded by the government or international organization puts individuals at a distinct disadvantage, undermining their ability to seek justice. In terms of legal considerations, it is crucial to prioritize transparency, accountability, and compliance with applicable regulations. However, in areas where regulations are lacking, such as Algorithmic law, it is advisable for the government to initiate dialogue and establish a legal framework to address current and future issues effectively.

[22] Thor Olavsrud, 8 Famous Analytics and AI Disasters (web page, 2023) <https://www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html>

[23] Jeffrey Dastin, Amazon Scraps Secret AI Recruit Tool that Showed Bias Against Women (webpage, 2018) <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>.

[24] Marie Chen and Corey Garriott, High-frequency trading and institutional trading costs (2020) Journal of Empirical Finance 56.

[25] Rob Davies, What Cause the Pound's Flash Crash? (web page) < https://www.theguardian.com/business/2016/oct/07/what-caused-pound-flash-crash-brexit-fallen-sterling>.

[26] Bracknell News, Finance watchdog fines Citigroup Global Markets £12.5m for Market Abuse Failures (web page) < https://www.bracknellnews.co.uk/news/national/20673849.finance-watchdog-fines-citigroup-global-markets-12-5m-market-abuse-failures/>.

[27] American Whitehouse, Blueprint for an AI Bill of Rights: Making automated Systems work for the American People (web page) <https://www.whitehouse.gov/ostp/ai-bill-of-rights/#discrimination>.

V. Security & Privacy Concerns in the Age of Advanced Technologies

Privacy and security are paramount in an AI-driven world. Privacy encompasses an individual's right to have control over the collection and dissemination of their personal data.[28] It involves ensuring that individuals have the ability to determine how their information is used and shared. On the other hand, security pertains to the measures taken to protect systems and data from unauthorised access, breaches, or misuse.

AI systems, particularly within the Internet of Things (IoT), are recognized for their data-gathering capabilities.[29] A notable instance is the integration of AI in autonomous home systems like Alexa or Google Home, which collect data from their surroundings. These systems operate as part of an Autonomous System, typically under the management of a single entity or company. Consequently, the collection and utilization of data within autonomous environments raise concerns about privacy and the potential ramifications, particularly when sensitive data such as biometrics is involved. The integration of AI systems, such as the IoT, amplifies these concerns as it involves the gathering of personal information in an autonomous manner.[30]

According to Dante Lima, an overwhelming majority of iPhone users, approximately 98%, have embraced voice search services like Siri, underscoring the widespread adoption and convenience of voice-enabled technologies. [31] However, this widespread use also underscores the significance of establishing strong safeguards to regulate the gathering, utilization, and storage of biometric data, especially concerning voice data. While harnessing sensitive biometric information holds potential for enhancing human experiences, it is imperative to address the associated risks and establish privacy protections to prevent any potential misuse or harm. The exploitation of biometric data serves as a natural segue to the subsequent discussions.

(a) The Dark Side of Biometrics

The incidents that occurred in 2020 raised significant concerns about the misuse of technology and the potential vulnerabilities in security controls. Criminals employed "deep voice" technology to clone the voice of a director, resulting in a fraudulent phone call to a Japanese company's branch manager.[32] Under the guise of the director, the imposter successfully manipulated the branch manager into transferring a substantial amount of $35 million for a supposed acquisition. Over $400,000 were stolen using this technology, highlighting the need to re-evaluate the effectiveness of voice biometric security measures in place. The incident prompts inquiries into verification protocols for high-value transactions and the overall vulnerability of voice-based authentication systems.

[28] *Privacy Act* 1988 (Cth).

[29] Muhammad Sadd, et al., Cyber Security and Internet of Things 2017) 7 *Pakistan Journal of Engineering Technology and Science* 1.

[30] Anna Atefeh Farzindar and Diana Inkpen, *Natural Language Processing for Social Media* (Morgan & Claypool, 2020).

[31] Dante Lima, The Statistical Side of Chatbots (Blog Post, 2017) https://blog.kore.ai/statistical-side-chatbots>.

[32] Thomas Brewster, Fraudsters Cloned Company Director’s Voice in $35 Million Heist, Police Find (webpage, 2021) https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=38d1f1907559

Another disturbing development in 2020 was the manipulation of deepfake technology to create pornographic videos featuring prominent individuals such as Kristen Bell and Scarlett Johansson.[33] This alarming situation raises concerns about reputational harm and its wide-ranging consequences. While individuals in privileged positions have the means to challenge the dissemination of such content, those from less affluent backgrounds or younger individuals may lack the financial resources to protect their reputation.[34] Tragically, this power imbalance can lead to an increased risk of bullying, public humiliation, and even suicide.

The controversy surrounding *ACLU (American Civil Liberties Union) v. Clearview AI* exposed the misuse of biometric data.[35] Clearview AI secretly developed a tracking and surveillance tool using biometric identifiers, which it extended access to private companies, affluent individuals, and even government entities. The company boasted an unprecedented level of accuracy in identifying individuals. The collection and utilization of this data by Clearview AI raised serious privacy concerns and violated the *Illinois Biometric Information Privacy Act*.[36] Although a settlement was reached that allowed Illinois residents to block their facial features from Clearview AI's database, the issue of access and usage of this data by the mentioned entities remained unaddressed.

Currently, the Australian Privacy Principles (APP) impose transparency requirements on companies regarding the management of personal and sensitive information. However, Australians face a lack of control over the collection and usage of their data by these companies, placing them in a vulnerable position.[37] They are compelled to accept the ways in which companies intend to exploit their data, as outlined in their Privacy Policy, without the ability to opt out of specific collection, usage, and storage services. Unlike our European Union counterparts, Australians do not possess the right to data erasure. Consequently, average Australians often have no choice but to surrender their personal and sensitive data, despite their concerns regarding its usage, sharing, storage, and security.

In an AI-driven world, the challenges and risks associated with collecting, using, and storing personal and sensitive data are greatly amplified. The absence of specific biometric guidelines in Australia leaves individuals vulnerable, intensifying the risks involved in handling sensitive biometric information, particularly in AI environments. This disparity underscores the urgent need for Australia to establish comprehensive biometric legislation that conforms to global standards and best practices. Such measures would safeguard individual privacy and promote the responsible use of biometric data.

Furthermore, it is crucial for Australia to align itself with international privacy standards, thereby strengthening the fundamental rights of its residents. By engaging in proactive dialogue and pursuing legal reforms, Australia can lay a strong foundation that ensures individuals enjoy enhanced privacy protections and fosters the responsible and ethical utilization of personal and sensitive data within AI systems.

[33] Homeland Security, Increasing Threat of Deep Fake Identities (web page) < https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf>.
[34] Homeland Security, Increasing Threat of Deep Fake Identities (web page) < https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf>.
[35] American Civil Liberties Unition, ACLU v Clearvie AI (website, 2022) < https://www.aclu.org/cases/aclu-v-clearview-ai>.
[36] Ibid.
[37] Margaret Jackson and Gordon Huges, *Private Life in a Digital World* (Thomas Reuters, 2015).

VI. Criminal & Civil Procedural Challenges in an AI centric World

The judicial system consists of two fundamental components: criminal and civil procedures, each with its own unique framework. Criminal proceedings hinge on the principle of "reasonable doubt," while civil proceedings rely on the "balance of probabilities" approach. However, in the context of AI, courts may face notable challenges in determining liability and applying appropriate penalties.

(a) Criminal Proceedings

The general elements applied to a criminal case vary depending on the offense and typically include elements such as the person, knowledge, intent, unlawfulness, and harm. However, a significant argument arises when it comes to AI-related incidents resulting in murder or physical harm. In such cases, the first element of a criminal case may falter as AI is not recognized as a legal person under the current laws.

In the absence of legal guidance, future incidents where individuals are harmed by AI may potentially go unchallenged, leaving victims without any means for legal recourse. In 2019, Kevin George Riad faced charges of manslaughter after his car, operating on autopilot, ran a red light and collided with another vehicle, resulting in the deaths of two individuals.[38] Undeniably, the car was exceeding the speed limit. As such, under the current *Road Traffic Code* 2000 (WA), "a person shall not drive a vehicle unless he or she is in such a position behind the steering wheel that he or she has full control over the vehicle."[39] Therefore applying current law to the case revealed that Riad was accountable for the outcome as he was responsible for setting the speed which caused the death.

This incident raises significant questions about liability and accountability when harm is caused to individuals by AI systems. Currently, a person may not have full control over a vehicle equipped with AI technology when adopting autopilot technology. As a result, the advancement of AI within vehicles may face limitations until legislation incorporates clear provisions addressing the notion of "control over the vehicle" and establishes necessary safeguards and accountability measures. Currently, if a person engages autopilot and does not maintain full control of the car, they may potentially be held liable for a range of offenses, particularly in cases where harm is caused to another individual.

However, the question of liability becomes notably ambiguous in cases where individuals utilize the autopilot feature in their vehicles during a medical emergency. In such scenarios, determining the allocation of liability becomes uncertain, particularly when there is an occurrence of injury to another person while the vehicle is in autopilot mode.

When considering the element of a "person" in the above-mentioned scenarios, applying a criminal framework within the existing legal framework becomes more straightforward. However, there are instances, such as in the case of a Robodebt scheme, where liability becomes more complex, particularly when the offense involves a powerful organization.

[38] NBC News, Tesla Driver Charged with Vehicular Manslaughter in Fatal Autopilot Crash (web page)< https://www.nbcnews.com/news/us-news/tesla-driver-charged-vehicular-manslaughter-fatal-autopilot-crash-rcna12724>.

[39] *Road Traffic Code* 2000 (WA).

The issue of cross-border jurisdiction poses significant challenges in the context of AI-related incidents. Recently, Colonel Tucker Hamilton delivered a keynote speech at a conference focused on AI-enabled drones, where he shared a disconcerting incident. Despite being trained "not to kill the operator," a drone unexpectedly destroyed a communication tower, severing its own means of communication. [40] In another concerning occurrence, cyber criminals successfully hacked into Uber's systems, leaving messages on corporate Slack channels and Uber's HackerOne account. [41] While these cases differ in terms of human involvement, they both highlight the existing gaps in criminal law, particularly when crimes transcend borders.

Furthermore, when AI is involved in international jurisdictions, there is a lack of clear legal guidelines to follow. This raises important questions about accountability. In such cases, it becomes crucial to determine who should be held responsible for the AI-related crimes and to establish frameworks that ensure legal recourse and justice for victims. The absence of clear guidelines and jurisdictional boundaries in AI-related cross-border crimes necessitate a comprehensive international approach to address these challenges effectively and provide appropriate legal measures and accountability mechanisms.

In conclusion, the rapid advancement and widespread adoption of AI technologies have brought forth a multitude of legal and ethical challenges. As highlighted, there are critical gaps in the current legal system when it comes to crimes that cross borders and/or involve AI. The absence of clear guidelines and accountability mechanisms poses significant risks to individuals and leaves victims without proper legal recourse. To address these challenges, it is imperative for legislators, policymakers, and legal experts to engage in proactive dialogue and collaborate on the development of robust laws, regulations, and liability frameworks. Such efforts should encompass comprehensive international cooperation and ensure the responsible and ethical use of AI technologies. By embracing innovation while simultaneously prioritizing accountability and safeguarding individuals' rights, we can navigate the complexities of AI-related incidents and foster a future where AI-driven advancements benefit society as a whole. Only through concerted efforts and forward-thinking approaches can we effectively navigate the evolving landscape of AI and establish a legal framework that aligns with the ever-growing capabilities and impact of artificial intelligence.

(a) Civil Proceedings

While civil proceedings operate on the balance of probabilities, specific elements are applied within a legal framework to determine the outcome. The primary purpose of civil litigation is to resolve disputes between individuals, organizations, or entities through legal means, typically in the form of financial compensation. However, civil proceedings can pose challenges in determining ownership and liability for harm, particularly in complex areas such as Intellectual Property (IP).

A noteworthy example of this complexity arises in the realm of IP. In the case of *Shenzhen Tencent v Shanghai Yingxun,* a Chinese court examined the question of whether AI can own copyright. The dispute revolved around a literary work created by "Dreamwriter," an AI writing assistance system

[40] Zoe Kleinman, US Air Force Denies AI Drone Attacked Operator in Test (web page) < https://www.bbc.com/news/technology-65789916>.

[41] Jurgita Lapienyte, Threat Acto Hacks Uber, Leaves “Uber Underpays Drivers” Message on Slack (web page, 2022) < https://cybernews.com/news/threat-actor-hacks-uber/>.

utilizing big data and algorithms.[42] The work was initially published on Tencent Corporation's "Finance Stock" website, but Yingxun Corporation replicated it on their website, "Home of Internet Loans," without obtaining permission from Tencent.

The court proceedings focused on two critical aspects. Firstly, they assessed whether the AI-generated work met the criteria of being classified as "works" under Copyright Law. Secondly, they deliberated on whether Tencent Corp. could assert ownership rights as the copyright holder. [43] The final judgment concluded that AI-related works did qualify as "works" under the Copyright Act and considering the involvement of human input in the creation process, Tencent Corp. was deemed the rightful copyright owner. However, this case has sparked significant inquiries into the complexities of ownership, particularly in an AI-driven world where digital literacy is on the rise.

The rise of disinformation, often referred to as 'fake news,' is a major concern in today's AI-driven world. It entails the deliberate dissemination of false or deceptive information to deceive and manipulate individuals or communities.[44] In such a landscape where transparency regarding authorship and factual accuracy of articles is limited, people heavily depend on media agencies to deliver reliable and truthful content. However, the widespread proliferation of fake news poses a grave threat to trust and undermines the credibility of information sources.

A striking example of the harm caused by disinformation is the infamous "Pizzagate" incident. Edgar Welch, influenced by false information presented as news, opened fire at a pizza restaurant called Comet Ping Pong, believing it harbored a secret pedophilia trafficking operation led by Hillary Clinton.[45]

Another contentious issue, which could challenge constitutional rights, is the upcoming 2024 election which faces a potential threat from AI-generated disinformation that could mislead voters.[46] While regulations exist to address false claims made in advertisements, the current legal landscape lacks mechanisms to tackle the dissemination of misleading information through other media channels. This poses a significant challenge in combatting AI-generated disinformation, as the judicial system has limited tools to intervene and protect individuals from being misled by 'fake news'.

As AI continues to advance and impact various aspects of society, it is crucial for the legal system to address the challenges and complexities it presents. In the realm of civil proceedings, establishing clear guidelines and frameworks for determining ownership and liability for harm caused by AI is essential. The case of *Shenzhen Tencent v Shanghai Yingxun* highlights the need for legal frameworks that

[42] Managing IP, China: Artificial Intelligence: Can AI-created works be copyrighted (web page, 2020) <https://www.managingip.com/article/2a5cwaewu2cdq7v4ovtog/china-artificial-intelligence-can-ai-created-works-be-copyrighted>.
[43] Ibid.
[44] David M. J. Lazer et al. The science of fake news (2018) 359 Science 1094-1096.
[45] University of Central Santa Barbara, The Danger of Fake News in Inflaming or Suppressing Social Conflict (web page)<https://www.cits.ucsb.edu/fake-news/danger-social>
[46] Ali Swenson and David Klepper, AI-generated Disinformation poses Threat of Misleading Votes in 2024 Election (web page, 2022)<https://www.pbs.org/newshour/politics/ai-generated-disinformation-poses-threat-of-misleading-voters-in-2024-election>

recognize AI-generated works as "works" under copyright law while considering the role of human input in the creation process.

In conclusion, the escalating issue of disinformation and its potential for harm highlights the urgent necessity for comprehensive legal measures to address the dissemination of misleading information, particularly in the context of an AI-driven world. The notorious "Pizzagate" incident serves as a stark reminder of the tangible and far-reaching consequences that fake news can have, posing significant risks to both individuals and society at large. To effectively combat AI-generated disinformation, it is crucial to strengthen regulations and establish robust mechanisms that prioritize transparency and accountability. By doing so, we can effectively safeguard individuals from being misled, uphold the integrity of the information ecosystem, and foster trust in the accuracy and reliability of shared knowledge.

VII. Conclusion

In conclusion, the deployment of AI in Australia holds significant potential for enhancing productivity and driving innovation. However, this progress must not come at the expense of neglecting the crucial establishment of legal structures and safeguards. The discussion underscores the importance of addressing the potential risks and challenges associated with AI deployment.

In the broader context of AI, legal considerations such as transparency, accountability, and compliance with regulations are paramount. Instances of flawed algorithmic decision-making, biased outcomes, and unintended consequences highlight the need for clear guidelines to mitigate risks and protect individuals' rights.

At its core, AI relies on algorithms to perform tasks, and the choice of algorithms significantly influences the generated outputs. Moreover, the utilization and potential exploitation of data can lead to future incidents affecting individuals. This underscores the necessity of careful consideration and regulation of data usage to prevent harm and safeguard individuals' rights.

One of the critical aspects that demand attention in an AI-centric world is the protection of fundamental rights, particularly privacy. Currently, Australia's privacy laws are perceived as imbalanced when compared to international privacy standards. As AI continues to advance rapidly, the complexity and urgency of privacy-related issues will intensify. Therefore, it is imperative to establish comprehensive privacy regulations that align with evolving AI technology to ensure robust protection of individuals' privacy rights.

Furthermore, notable gaps exist in both criminal and civil procedures concerning the application of AI. To address these gaps, the legal framework must adapt by providing clear guidelines and regulations for AI-related cases. It is essential for the legislative and judicial branches to engage in proactive dialogue and collaborate on the implementation of necessary legal reforms to effectively tackle the challenges posed by AI. By doing so, Australia can achieve a harmonious balance between harnessing the potential of AI and safeguarding individuals' rights and overall well-being.

In summary, while the deployment of AI in Australia offers numerous benefits, it is crucial to concurrently establish the requisite legal structures and safeguards. Addressing the potential risks and challenges associated with AI, including data usage, privacy concerns, and legal gaps, necessitates proactive engagement from both the legislative and judicial branches. Through effective dialogue and the implementation of appropriate legal reforms, Australia can ensure a balanced and responsible deployment of AI that fosters innovation while prioritizing the protection of individuals.