DOI: 10.53116/pgaflr.2021.2.3

Algorithms of Machines and Law: Risks in Pattern Recognition, Machine Learning and Artificial Intelligence for Justice and Fairness

Michael Losavio[*]

[*] Associate Professor, University of Louisville, Department of Criminal Justice, e-mail: michael.losavio@louisville.edu

Abstract: Pattern recognition, machine learning and artificial intelligence offer tremendous opportunities for efficient operations, management and governance. They can optimise processes for object, text, graphics, speech and pattern recognition. In doing so the algorithmic processing may be subject to unknown biases that do harm rather than good. We examine how this may happen, what damage may occur and the resulting ethical/legal impact and newly manifest obligations to avoid harm to others from these systems. But what are the risks, given the Human Condition?

Keywords: pattern recognition, artificial intelligence, governance, management, justice, ethics, human condition

1. Introduction

Pattern recognition (PR) and artificial intelligence (AI) are machine systems for finding or inferring patterns and relationships in data. The power of these systems and their deployment across multiple social, commercial and government domains impacts everyone. But with much technology in human history, examination of ethical, human and legal impacts of PR/AI lags, ignoring risks to people's lives. The risks of unintended injury from the systems is significant. In the area of facial recognition, both Amazon and IBM have withdrawn their AI facial recognition systems from law enforcement use due to concerns about errors. These errors might lead to wrongful arrest or worse.

To detail the interrelationship of law with PR and AI in society, consider how facts map to law. Figure 1 details the fact elements necessary for the offense of reckless homicide, for which a person is guilty if they unintentionally but with reckless disregard of the dangers kill someone.

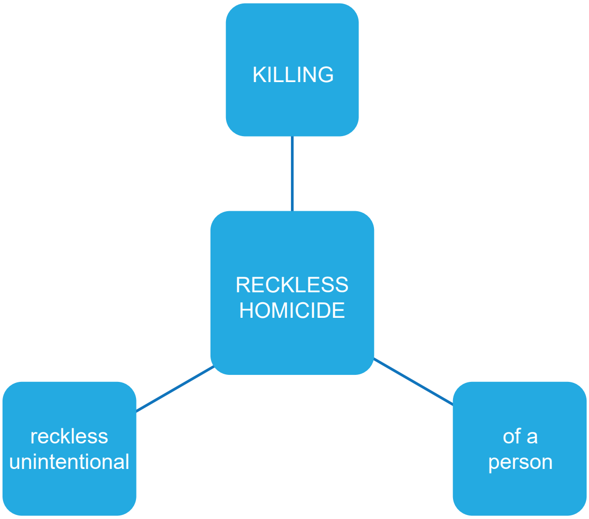

Figure 1.
The fact elements of reckless homicide from AI controls

Source: Compiled by the author.

If the AI system contributes to any of these elements, and all are present, those who designed, distributed and used that system may be criminally liable for the death. Table 1 deconstructs outcomes from AI control systems for medical treatment devices causing unintentional injury.

Table 1.
Potential criminal liability for flawed AI-controlled system

AI-controlled Medical Device for Radiation Treatment of Cancer Patients			
Mental state of the designer, seller, user	Object of injury	Type of injury	Criminal Liability?
Designer knows of danger incorrect treatment but fails to do standard software testing	Person receiving treatment	Death	Yes
Seller knows of injuries to others but continues to sell device	Person receiving treatment	Death	Yes
System user learns of injuries to others but continues to use device	Person receiving treatment	Death	Yes

Source: Compiled by the author.

Advances in AI have contributed to growing interest in industry, government and education. Innovative applications and industries and products allow the use of AI to automate many endeavours, such as business processes, services, manufacturing, transportation and entertainment. But the application of AI has, in some cases, proved to be flawed increasing the risks to security, privacy and personal safety. A growing interest in AI safety is now a branch of ethics and technology of its own. This is matched by discussion and litigation as to liability for the injuries resulting from flawed AI, as discussed below.

2. People, patterns and artificial intelligence

Artificial intelligence and pattern recognition systems are technological tools for people. The effect of such systems should comply with systems of rights and responsibilities. These together form a legal-technical ecosystem in the world. Artificial Intelligence may reveal much previously private and hidden inferences. One of the first computational-mediated devices for the collection and analytics of data, upon court review for violation of fundamental rights of citizens, produced speculation that these technologies might change the relationship between government and the governed.[1] That change may not necessarily be for the better.

2.1. Policies, procedures and regulation for artificial intelligence and pattern recognition

Legal implications, compliance and utility for AI and PR are intricate. Analysis of the technology, possible injuries and regulation, present and future, are essential. Injuries once minor and dismissed through service level agreements become grounds for liability under various legal doctrines, especially that of products liability that holds those creating a "defective" product injuring others must pay for those injuries regardless of any agreement to the contrary. Injury to others calls for legal regulation. The technologies of AI and PR are integrated into administrative-cultural-legal frameworks.

There are a variety of new issues with AI for digital forensics, evidence recovery, provenance and source discovery, and validation may require application of multiple tests to components of an evidence object. The systems and protocols for security and privacy in electronic objects, metadata, source and storage devices and transactional data may both support forensic discovery but also counter forensic efforts.

The life or death aspect of police power has led a group of mathematicians to call for ending collaboration with police departments and to publicly audit policing algorithms (Aougab et al., 2020). Calls have come out to limit the use of AI as matters of policy, especially in policing; the Government Accountability Office, Science, Technology Assessment and Analytics team of the United States is evaluating law

[1] *United States v. Jones,* 574 US ___ (2014).

enforcement AI systems as to reliability (Uberti, 2020). Legislation is pending in the U.S. Congress to set standards for the country on forensic algorithms that would also negate any trade-secret privileges and systems used to block examination of the algorithm source code. The Global Partnership on Artificial Intelligence of fourteen countries and the European Union, with support from the OECD (2020) and UNESCO, has formed to guide "responsible development and use of AI" while respecting human rights, stating:

> Recognising the need for cooperation at international level if we are to tap the full potential of artificial intelligence (AI) and ensure that it is of benefit to all citizens while respecting democratic values and the primacy of human beings, the founding members of the Global Partnership on Artificial Intelligence (GPAI) mean to encourage and guide responsible development of AI based on human rights, inclusion and diversity while fostering innovation and economic growth (Gouvernement de France, 2020).

Calo posits policy for AI must address challenges to:

- justice and equity
- use of force
- safety and certification
- privacy and power
- taxation and displacement of labor (Calo, 2018).

AI policy issues are under discussion early in its implementation, creating the opportunity to implement policies before damage is done.

Global concerns with the fair, just and reliable use of AI arise from the sheer wealth of invasive power and evidence offered and the sensors of the Internet of Things, and must be addressed at a policy level. The power of AI gives it a central place in security preparations and forensic examinations across the spectrum, but these must be implemented under the rule of law, respect for human rights and our need for justice. We discuss factors that must be addressed for proper and reliable use of AI, PR and machine learning.

2.1.1. Case Study of artificial intelligence and human impact: Los Angeles Police Department Laser and PredPol predictive policing deployments

Los Angeles, California, has the third largest police department in the U.S. The Los Angeles Police Department adopted a number of computational and algorithmic systems to help guide its policing. One priority was interdiction of violent offenders, including by resource allocations to crime "hotspots". There were concerns that AI/algorithmic systems may reflect inherent racial biases in the programming and deep learning/machine learning analysis of historical databases. There were further concerns that these systems were not validated through empirical testing and analysis, a reliability review normally required for the forensic use of evidence and inferences in legal proceedings.

A review and audit of the systems was made by the Inspector General of the Los Angeles Police Department (Office of the Inspector General, 2019). The systems reviewed included a Predictive Policing system (PredPol). That review found, among other things that the officers – the human component of the system – were not consistent in their application of criteria leading to their conclusions regarding criminal activity. This led to the suspension in the use of at least one of these tools and its tracking database.

PredPol and its location-based predictive policing were found to have discrepancies in data collection such that program effectiveness could not be evaluated. PredPol modelled officer visits to areas matched against outcomes. Ideally this would connect enforcement activities to community impact. Analysis of these systems could not establish that they were, in fact, effective. Rather it led to a set of recommendations to assure greater reliability; these included formal written protocols that would:

- articulate goals and expectations for the program
- provide clear delineation of selection criteria
- remove potential bias elements through requirement of minimum numbers of targets identified
- provide notice and corrective systems for people identified by the system
- provide process for removal from the program target list
- articulate mandatory program activities
- articulate prohibited program activities or limitations on action

Reform of database and system design required collection of further information on why a person was targeted, date of admission to the database, dates of active or inactive status and reporting information on the individual. Further data was needed on the nature of any Los Angeles Strategic Extraction and Restoration program directed activities and the results of that activity and the source of updates regarding target individuals. Retention policies on data and reports from the program were required to provide for review of activity; guidance language in activity bulletins generated should be reviewed by the Los Angeles City Attorney. A consistent training program for all users of the program needed to be developed and implemented. An audit system must be in place to provide oversight of the data collection and utilisation of these systems for public safety.

The Inspector General noted that although immensely powerful, the melding of these systems clearly created risks where there is not adequate preparation or system validation. In the area of public safety this can be particularly dangerous for the identification of someone as a violent offender means that police in encounters with them may come with the anticipation of violence and related increase in risk.

2.2. The ethics of information technology and artificial intelligence

Artificial intelligence ethics has become an area of its own, extending from philosophical discussions of personal autonomy of AI into dual tracks regarding ethical obligations to deal with it. The Letter to AMS called for boycott of police collaboration and called for the inclusion of learning outcomes in data science classes that cover the ethical, legal and social implications of AI systems (Aougab et al., 2020). The Association for Computing Machinery and IEEE-CS issued a joint Software Engineering Code of Ethics and Professional Practice applicable to AI development (Gotterbarn et al., 1997). The Code, though high-level, mandates that "software engineers shall act consistently with the public interest".

More granular ethics analyses have identified outcomes to be addressed. Chalmers proposed the need for a "leakproof" containment system for AI development that, at its most extreme, isolates AI systems until their full capabilities are known (Chalmers, 2010).[2] Yampolskiy (2012) has addressed this in the context of the safety of people, not simply that of machines.[3] The general framework for approaching ethical analysis with Information and Communications Technologies (ICT) may apply specifically to AI and PR systems. One such framework, built upon that and used for human subject research generally, was set out in the Menlo report (Keneally, 2012).

The Menlo report proposes a framework for ethical guidelines for computer and information security research based on the principles set forth in the 1979 Belmont report for human subjects research. The Belmont report had as its primary focus biomedical research on human subjects and the ethics regarding the treatment of those human subjects. In the U.S. it has become the foundation for the "common rule" applicable to all human subjects research, from biomedical sciences to social sciences. It acknowledges that there are new challenges resulting from interactions between humans and information and communications technologies (ICT). ICT research contexts contend with ubiquitously connected network environments, overlaid with varied, often discordant legal regimes and social norms. The lack of a tradition of analysis of the ethical implications of ICT research itself creates the potential for risk; both in the context of the sometimes horrific history of traditional human subjects research. The evolving landscape of ICT research stakeholders, especially with AI/machine learning, require special attention.

2.2.1. The Menlo report

The ICT research Menlo report proposes three core ethical principles, three of which derive from the Belmont report: 1. respect for persons; 2. beneficence; and 3. justice. To these Kantian concerns connect the additional principle "respect for law and public interest", a recognition of how the novelty of these technologies and the lack of

[2] See also Yampolskiy (2012a).

[3] See also Yampolskiy & Fox (2012).

a tradition of care can lead researchers and developers to create things that may, however unintentionally, hurt others. The goal of the report is to propose standard methods for ICT research for:

- identification of stakeholders and informed consent
- balancing risks and benefits
- fairness and equity
- compliance, transparency and accountability

These principles and applications can be supported by outside oversight and internal self-evaluation tools. The starting point of the analysis is to identify "stakeholders" in the process, being those people who have an interest or are impacted by the implementation in the world of the ICT systems developed. These would include:

- researchers
- human subjects, non-subjects, ICT users
- malicious actors
- network/platform owners and providers
- government/law enforcement
- government/non-law enforcement (e.g. public services)
- society collectively

Researchers, developers and users have to look at and consider respect for the people impacted by the systems. This includes recognition of the personal autonomy of the subjects as well as protection of those with reduced autonomy (ill, handicapped, youth, inmates). The idea of informed consent means that the subjects impacted by any system are made aware of the activities, risks, benefits of the system and have a choice whether to proceed with it or not.

The principle of "respect for law and public interest" is a protective measure for the subjects of the systems and the developers/users themselves. It entails the principles of compliance and transparency/accountability:

- compliance
  - identify laws, regulations, contracts and other private agreements that apply to their research
  - design and implement ICTR that respects these restrictions
- transparency and accountability
  - mechanism to assess and implement accountability
  - responsibility for actions and outcomes

There are a variety of existing ICT Ethics Codes that can serve as guides for the evolution of practices, even as they do not have particularly significant enforcement or regulatory powers themselves. Those codes of ethics include:

- IEEE/ACM Codes
- Association of Internet Researchers
- National Academy of Sciences
- SAFE/LPS SA/USENIX – joint System Administrators Code of Ethics

- responsible disclosure guidelines – National Infrastructure Advisory Council
- Internet Advisory Board Guidelines – IETF

One recent example of this is a collaboration between Google and Apple Inc. in the development of an app for contact tracing amidst the ongoing coronavirus pandemic. The ethical issues raised by the system and its ability to bypass privacy of citizens are addressed by the voluntary nature of the use of the application, where the users are informed of how the system works and may choose to use it or not to help provide better hygiene regarding people with whom they have been in contact.

Thus with AI research and implementation those involved, from designers to system users, should engage in the following analysis to better know that what they are doing is ethically correct, and also use it as a potential bellwether for legal liability:

- identification of stakeholders and informed consent
- balancing risks and benefits
- fairness and equity
- compliance, transparency and accountability

The analytics injury to life and person must consider injuries:

- life and person
  - loss of life, physical/mental injury to person
- liberty and personal autonomy
  - privacy rights and control of personal information
  - reputation and public image
  - freedom of action and person
- property
  - rights and interests
  - informational
  - costs of remediation and recovery

2.2.1.1. Case Study of a proactive analysis – The Axon Artificial Intelligence and Policing Technology Ethics Board

In contrast to post-hoc, after-the-fact analyses, the Axon police technology company, testing AI systems for law enforcement, impanelled an ethics board *prior* to system deployment. The panel was to examine the risks and appropriateness of AI technology in public safety and security. The panel set out a series of issues to be examined that are generally applicable for evaluating AI technology and are instructive as *a priori* vetting of an AI/PR implementation:

1. What is the specific problem to be solved?
2. How important is the problem?
3. How certain is it that the technology will address the problem?
4. May there be unintended or secondary benefits:
   - minimise criminalisation of low-level offenses

- additional control and protection of personal data
- mitigation of racial and/or identity bias
- improved transparency or public trust
- better compliance with U.S. constitutional requirements
- other societal benefits
- guidance in assessing costs?

5. Can the technology be used or misused in unanticipated ways?
6. Will it lead to greater criminalisation or to policing in counterproductive ways?
   - 6.1. Will the technology impact personal information privacy?
   - 6.2. What is the data captured, retained, owned, accessed, protected?
7. Does the technology implicate potential biases, especially racial or other identity factors, whether in design or use?
8. Does the technology create transparency-related concerns with the public?
9. Does the technology risk, directly or indirectly, violations of constitutional or legal rights?
10. Are there other potential social costs that have not been considered, such as impact on specific groups, "mission creep", historical issues, industry influence, global human rights? (First Report of the Axon Artificial Intelligence and Policing Technology Ethics Board, June 2019.)

The preliminary analysis of AI and facial recognition technology found serious concerns. The ability to capture, match and identify facial data may be hampered by issues of false positives and false negatives, due to issues of gender, age and race as well as the quality of imagery. The use of body camera imagery raises particular issues as they may lead to targeting as a suspect or arrest. This was a concern under American constitutional law and by governments around the world.

The ethics board concluded facial recognition technology under the AI systems in place was not reliable enough to ethically justify its use against body camera data and if it would *ever* be ethical to use it without additional support. Greater accuracy and consistent performance across multiple identity groups would be required to justify its use.

Validation of the algorithms for facial recognition would require a rigorous "false positive – false negative" assessment rather than the more amorphous concept of accuracy. The measurement of the "false positive – false negative" rates would better determine what is needed or permissible for use for law enforcement purposes. Use of such systems should be predicated on evidence-based evaluation of clear benefits, not on anticipated or speculative ones. The ethics board refused to endorse the development and deployment of facial recognition technologies that can be customised by the end users. Such customisation would allow systems to deviate from performance testing results as well as allow the introduction of inconsistent data, analysis and use/misuse. These inconsistencies might be difficult if not impossible to detect posing a challenge to the judicial system to properly oversee their application.

In express acknowledgment that the deployment of AI against diverse data collection systems fell within a broader ecosystem of social and legal constraints, the ethics board said that the use of such AI-mediated technology should first be vetted through *"open, transparent, democratic processes, with adequate opportunity for genuinely represented public input and objection".* To be effective, this would require cost-benefit analyses that match the power and limits of the technology against "the realities of policing in America and in other jurisdictions". The board noted that this was only the first report on what would be an ongoing evaluation of AI and ethical use of police technology. It hoped that its work would serve as a general guide for all technology developers creating and providing those systems.

2.3. The law of IT and AI

The use of analytics in multiple domains offer exceptional benefits. But data modelling and statistical inference challenges social and legal bounds of privacy, personal autonomy and personal security. Particularly when the analytical inferences go wrong or are wrongly used. The liability for the injuries produced may be civil with money damages and criminal with fines and imprisonment. Such a projection produces widely disparate opinions for predictive analytics across domains, such as its foundation for the future of policing (Davidson, 2019) to an illiberal system for predicting enemies (Deeks, 2018).

The facts of AI and predictive systems are part of a socio-technical system for governance that embraces human decisions, machine decisions and responsibility. Analytics and computing become ubiquitous in data sources and uses, such as the Internet of Things, the Smart City, analytics for everything from toll use to bread and butter, evolving standards, e.g. the national spatial data infrastructure, general data protection regulation (EU). The danger is that we operate the systems upon such meta-assumptions as our computational systems will be error free, our computational systems will be human mediated as to correct any errors, our computational systems will be too complex for the lawyers to figure out how to sue us.

The civil liability in data collection, analytics and disclosure embrace a number of areas depending on the injuries produced and the stakeholders and their roles in those injuries. These include: tort liability/products liability – mental state; infringement of civil rights/statutory liability – mental state; criminal liability – mental state; data collection, storage and transmission; analytics, algorithms, rendition, visualisation, intel, warrants; systems and users. For example, under U.S. law it is a civil liability to intentionally infringe the civil rights of citizens pursuant to the federal statute 42 USC §1983. This paralleled in U.S. federal criminal law 18 USC §242 which punishes for the wilful deprivation of civil rights under the colour of law. There are particular federal Constitutional (U.S.) concerns: Fourth Amendment (secure from unreasonable searches and seizures), Fifth Amendment (no deprivation of property or liberty without due process of law) and Fourteenth Amendment (equal protection of the laws and due process of law).

2.4. Case Study of law and artificial intelligence and pattern recognition: Analysis of government processes and injuries from artificial intelligence techniques

The lagging indicator nature of jurisprudence to reflect legal recognition of technological concepts can be seen with the Internet of Things, first described in 1999 (Makker, 2017). U.S. Federal Court analysis was fifteen years later and growing eight-fold five years later. The policy and judicial analysis of AI both guide and warn. Public safety is an essential public service and AI holds great promise in that domain. Some opine that AI is no longer science fiction but the future of policing (Davidson, 2019). It can more swiftly make determinations about people that impact their lives and liberties through misuse or error. It challenges social and legal bounds of privacy, personal autonomy and personal security. It is the interplay between human decisions and machine decisions that will impact people's lives. Defining responsibility for that impact is critical, just as Cathy O'Neil cautions great care in the use of these "weapons of math destruction" (O'Neil, 2016).

2.4.1. Case-based analysis – Robotic justice

The *Cahoo* et al. *v. SAS Analytics Inc.* et al. case[4] addressed accountability for flawed data analytics by a state entity contrasting fundamental legal obligations with AI/predictive analytics outcomes. Anyone violating the rights of citizens contrary to the U.S. Constitution may be prosecuted for civil damages (42 USC §1983) or criminal punishment (18 USC §242). The system at issue "robo-adjudicated" fraud in unemployment compensation claims. These "robo-adjudications" led to denial of benefits and significant penalties despite a 93 per cent error rate of "false positives" of fraud. The defendants' assertions that they were not liable were rejected and they were found liable for civil damages (money damages) to those injured. Those damages included deprivation of unemployment benefits and the after-the-fact seizure of people's assets, leading in some cases to eviction and bankruptcy.

No state shall "deprive any person of life, liberty, or property, without due process of law".[5] This was long established that people applying for and receiving unemployment compensation have constitutionally-protected property interests in unemployment benefits.[6] The Due Process Clause offers protection for those who show:

- that they have a property interest protected by the Due Process Clause
- that they were deprived of this property interest
- that the state did not afford them adequate pre-deprivation procedural rights

[4] *Cahoo et al. v. SAS Analytics Inc. et al.* No. 18-1296 (6th Cir. 2019).

[5] Fourteenth Amendment, §1.

[6] See *Goldberg v. Kelly* 397 US 254, 262 (1970).

The system MiDAS determined fraudulent conduct through automated processing of current and past applications, finding discrepancies in unemployment insurance benefits. The system determined if there was fraud. It did not check for errors in data sources or good-faith mistakes. It used an "income spreading" algorithm for averaging income across a fiscal quarter into every week regardless of any income; if it was reported no income for any of those weeks a fraud finding was made. No subsequent verification was performed, claimants were not told the reasons for the finding nor allowed to dispute the finding. The system automatically assessed penalties equal to four times the amount of unemployment benefits received or sought, driving some into bankruptcy.

A review of the fraud determinations found a 93 per cent error rate with no fraud. Human-mediated review was added, reducing the error rate to 50 per cent. Yet the system continued to be used and enforcement actions continued. The state defendants clearly violated markedly-established constitutional due process rights to challenge these wrongful determinations. This powerfully demonstrates both the damage from AI mediated systems and the failure of people to remedy that damage to others, even upon notice.

3. Future action

Concerning robo-adjudication in administrative agencies or police action in pursuit of public safety, the development and deployment of AI must be done as part of the much broader legal-technical eco-system. The proactive approach of Axon to conduct an analysis of AI deployment issues is the model to be followed. Major developers such as IBM and Amazon have chosen to follow that model before people are hurt. It is vital to measure the impact on personal safety, security and privacy before the implementation of such powerful systems.

Yemini (2018) notes that the irony of the modern Internet is that "[it] provides more expressive capacity to individuals than ever before, also systematically diminishes their liberty to speak". This is due to particular negative impacts from what should be the most amazing system for the information from lack of anonymity; and lack of inviolability. These apply with even more force to AI and predictive analytics. Computational systems enhance forensic systems in several ways (Franke & Srihari, 2007). These include the production of objective, reproducible analytical conclusions, visualisation and pattern recognition. But there are issues with the proper validation of computational forensic techniques to assure their reliability and the importance of a systematic approach to computational forensics, cooperation between forensic and computational scientists and continued peer-review and testing of computational forensic techniques.

A summary of concerns relating to probabilistic evidence is in the analysis of the trial court noted in the United States federal criminal case *United States v. Shonubi:*

> Several commentators have expressed particular concern about the use of explicitly probabilistic evidence in criminal cases. See, e.g., Ronald Dworkin, *Taking Rights Seriously* 13 (1977); Andrew von Hirsch, Prediction of Criminal Conduct and Preventive

> Confinement of Convicted Persons, 21 *Buff. L. Rev.* 717, 744-50 (1972); cited in Barbara D. Underwood, Law and the Crystal Ball: Predicting Behavior with Statistical Inference and Individualized Judgement, 88 *Yale L.J.* 1409, 1412 (1979); Saks & Kidd, supra, at 152; Tribe, supra; Nesson, supra; L. Jonathan Cohen, Subjective Probability and the Paradox of the Gatecrasher, 1918 *Ariz. St. L.J.* 627, 632; (rejecting use of statistics in criminal cases); Alex Stein, On the Unbearable Lightness of "Weight" and the Refoundation of Evidence Law 48-49 (forthcoming 1995, on file in the instant case) (arguing that the problem with "naked" statistical evidence in criminal cases is not that it is unreliable, but that its "weight" is insufficient to support conviction) [*United States v. Shonubi* 895 F. Supp. 460, 518 (E.D.N.Y. 1995)].

Yet little has progressed since this. Some see the Bayesian analysis as the future of computational forensics in a variety of fields. Validating this for accuracy, precision, testability, test results and error rate is essential to qualify them as competent evidence. Yet such a process may be difficult and possible only through a weighing of the testimony of competing and sometimes contradictory experts in the field. One example is that "explainable" AI is a minimum requirement for adequately vetting AI forensics within judicial fora, such as under Federal Rule of Evidence 702 (U.S.) for expert system evidence.

4. Conclusion

The deployment of AI/PR systems across every domain will make for more and more challenges and problems to be addressed. Anticipating those issues and at least attempting to remediate them will both save people from illicit injury and developers from unexpected punishment. Legislative efforts to build out frameworks for AI/PR recognition will continue and will guide AI development. It is critical that the technologists with knowledge of these systems both conform their work to those requirements. And it is equally critical that they inform those creating these regulatory frameworks of the reality and facts of AI systems so those frameworks encourage competent and effective AI development while limiting poor and harmful AI design.

References

Aougab, T. et al. (2020). Letter to American Mathematics Society Notices: Boycott collaboration to police. Online: https://bit.ly/312vLls

Calo, R. (2018). Artificial Intelligence Policy: A Primer and Roadmap. University of Bologna Law Review, 3(2), 180–218. Online: https://doi.org/10.2139/ssrn.3015350

Chalmers, D. (2010). The Singularity: A Philosophical Analysis. Journal of Consciousness Studies, 17(9–10), 7–65.

Davidson, R. (2019, August 8). Automated Threat Detection and the Future of Policing. US FBI Bulletin.

Deeks, A. S. (2018). Predicting Enemies. Virginia Law Review, 104(8).

First Report of the Axon Artificial Intelligence and Policing Technology Ethics Board, June 2019.

Franke, K. & Srihari, S. N. (2007, August 29–31). Computational Forensics: Towards Hybrid-Intelligent Crime Investigation. Proceedings of the Third International Symposium on Information Assurance and Security. Online: https://doi.org/10.1109/IAS.2007.84

Gotterbarn, D., Miller, K. & Rogerson, S. (1997). Software engineering code of ethics. Communications of the ACM, 40(11), 110–118. Online: https://doi.org/10.1145/265684.265699

Gouvernement de France (2020, June 17). Launch of the Global Partnership on Artificial Intelligence. Online: https://bit.ly/3r6jxTz

Keneally, E. et al. (2012, August 3). The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. Online: https://doi.org/10.2139/ssrn.2445102

Makker, S. R. (2017). Overcoming "Foggy" Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things. UMKC Law Review, 85(4), 895–915.

Office of the Inspector General (2019, June 12). Review of Selected Los Angeles Police Department Data-Driver Policing Strategies. Online: https://bit.ly/3cIfEvJ

O'Neil, C. (2016). Weapons of Mass Destruction. Crown Publishing.

Organization for Economic Cooperation and Development (2020, June 15). OCED to host Secretariat of new Global Partnership on Artificial Intelligence. Online: https://bit.ly/3l89BFl

Uberti, D. (2020, June 1). Algorithms Used in Policing Face Policy Review. Artificial Intelligence Daily, Wall Street Journal.

Yampolskiy, R. V. (2012a). Leakproofing the Singularity Artificial Intelligence Confinement Problem. Journal of Consciousness Studies, 19(1–2), 194–214.

Yampolskiy, R. V. (2012b). Artificial Intelligence Safety Engineering: Why Machine Ethics Is a Wrong Approach. In V. C. Müller (Ed.), Philosophy and Theory of Artificial Intelligence (pp. 389–396). Springer. Online: https://doi.org/10.1007/978-3-642-31674-6_29

Yampolskiy, R. V. & Fox, J. (2013). Safety Engineering for Artificial General Intelligence. Topoi, 32(2), 217–226. Online: https://doi.org/10.1007/s11245-012-9128-9

Yemini, M. (2018). The New Irony of Free Speech. Columbia Science and Technology Law Review, 20(1). Online: https://doi.org/10.7916/stlr.v20i1.4769