Artificial Intelligence and the Testing Industry: A Primer

A Special Publication from ATP

Authored by the International
Privacy Subcommittee of the
ATP Security Committee
July 6, 2021

Contents

OVERVIEW

This White Paper provides a high-level overview and definition of Artificial Intelligence ("AI"), use cases drawn from the testing industry, international standards and frameworks related to AI that share commonly accepted principles governing the appropriate responsible use of AI, and legal requirements for AI usage when personal information is processed. This Paper also describes specific risks arising from use cases in light of the standards and laws.

WHAT IS AI?

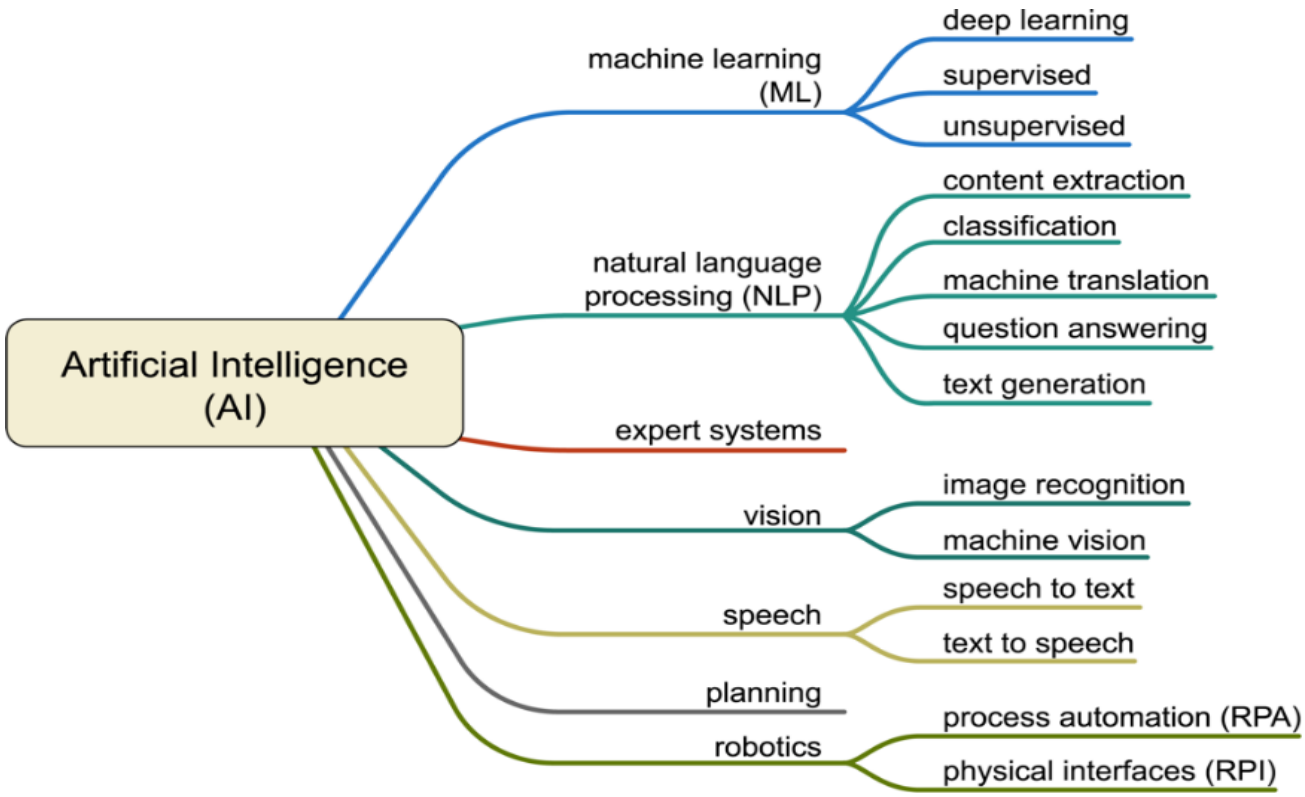
There is no easy answer to the question of what constitutes AI and understanding how it will impact society and the testing industry. Former IBM CEO Ginni Rometty has repeatedly opined that 100% of all jobs will change due to Artificial Intelligence (AI) in the next 5 to 10 years.[1] This means that everyone participating in the global economy will increasingly co-operate with, strategize using, and engage with AI-based or AI-containing systems. Therefore, it is critical to understand what artificial intelligence means, the acronym for which (AI) is so readily used.

In reality, AI is a complex, confusing, and misunderstood term. Testing organizations are often unaware of the role that AI already has in common activities, experiences, and interactions today – and of the importance for recognizing the increasing concerns and scrutiny about the use of AI. How did AI become so pervasive, and what is its future? To understand and address all of these questions, we first must understand what AI is.

[1] CNBC. www.cnbc.com/2019/04/02/ibm-ceo-ginni-romettys-soluton-to-closing-the-skills-gap-in-america.html.

A Historical Perspective[2]

Artificial intelligence, as a discipline of computer science, traces its origins to some of the first publications in the then nascent field of digital computing. One of the first papers to examine logic and intelligence was McCulloch's and Pitts' 1943 publication[3] of "A Logical Calculus of Ideas Immanent in Nervous Activity," in which they postulated that "…neural events and the relations between neurons in the neural network can be treated by means of propositional logic."



[2] Disciplines of AI Illustration created by Mike Sparling (©2021 Mike Sparling)

[3] W. S. McCulloch, W. Pitts. "A Logical Calculus of the Ideas Immanent in Nervous Activity"," in Bulletin of Mathematical Biophysics 5, pp. 115–133, 1943. https://doi.org/10.1007/BF02478259.

In a paper published in 1950 titled "Computing Machinery and Intelligence"[4] famed computer scientist Dr. Alan Turing posed the question, "Can machines think?" Turing developed not only methods for codifying intelligence, but also expressed the famous Turing Test, which is one method for measuring the intelligence of a conversational system.

In a 1959 paper titled "Some Studies in Machine Learning Use the Game of Checkers,"[5] IBM scientist Arthur Samuel defined artificial intelligence, and introduced the concept of machine learning, as "[a] Field of study that gives computers the ability to learn without being explicitly programmed." More recently Berkeley professor, and director of Google Research, Dr. Peter Norvig noted that:

"AI is all about figuring out what to do when you don't know what to do. Regular programming is about writing instructions for the computer to do what you want it to do, when you do know what you want it to do. AI is for when you don't."[6]

University of Toronto Professor, and Google Researcher, Dr. Geoffrey Hinton, who has been called "the godfather of AI" for his pioneering work on neural networks and deep learning, has said that "[t]he traditional concept of AI relied on logic and rules to program computers to think. Neural networks involve setting up computer systems to mimic the human brain, allowing them to learn."[7]

A Formal Definition

Related to the concepts described above, then, a definition of an AI system is one that perceives its environment and takes actions that maximize its chances of success in achieving an assigned task, outcome, or objective. An AI system can adapt to unforeseen circumstances by evaluating potential actions. The ability to evaluate actions (called "utility" in literature) is what differentiates AI from conventional computing.

---

[4] A. M. Turing, I. "Computing Machinery and Intelligence"," in Mind, vol. LIX, issue 236, pp. 433-460, October 1950, **https://doi.org/10.1093/mind/LIX.236.433**.

[5] A. L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers," in IBM Journal of Research and Development, vol. 3, no. 3, pp. 210-229, July 1959, **https://doi.org/2010.1147/rd.33.0210**

[6] Talati, A. (2018, September 12). CS 6601 Artificial Intelligence. Retrieved from Subtitles To Transcripts: **https://subtitlestotranscript.wordpress.com/2018/09/12/cs-6601-artificial-intelligence/**

[7] Gray, J. (2017, April 07). U of T professor Geoffrey Hinton hailed as guru of new computing era. Retrieved from The Globe and Mail: **https://www.theglobeandmail.com/news/toronto/u-of-t-professor-geoffrey-hinton-hailed-as-guru-of-new-era-of-computing/article34639148**

For example, if one is programming a car to drive from A to B, the "conventional computing way" is to program a set of instructions (e.g., "turn left, go forward, then turn left again"), which is only correct for a particular route from A to B. By comparison, the "AI way" is to program actions (e.g., "turn left", "go forward", "turn right"), include a utility (e.g., "what is the distance to the destination?"), and let the AI system adapt itself by analyzing if it will be closer to the destination after each action. Thus, using an AI system results in the selection of a route deemed to be the most efficient.

Machine learning (ML) is a subset of AI algorithms that have the capability of improving through experience. The process of learning happens when the ML system revaluates the assumptions built into its original coding by minimizing the discrepancies between its output (results derived from predictions based upon models or beliefs) and ground truth (known to be real based upon actual measurement or observation) data.

Consider an email spam filter for example. To implement an email spam filter, we would first train the ML system to extract features from emails (e.g., the sender of the email, the number of recipients, the subject line, the content, attachments, etc.). The ML system would then find the optimal combinations of features that allow it to mark emails as spam in a way that produces results that are as similar as possible to the original labels in the training data.

An Operating Perspective

Although definitions and concepts of AI may differ based upon the goals and the domain in which it is used, very simply, an AI system arrives at a prediction based upon one or more observations. At its core, an AI model will always return a prediction.

For example, the statement that a photograph is 97% likely to be a cat, or in the English language, the word that 85% of the time follows the words "this and" is "that" are both predictions and well within the capability of a narrow AI model. In these examples, the AI system may appear to know the English language or the taxonomy of small mammals, but in reality, the AI system has no understanding of English any more than it does of biology.

As advances in computer technology and storage have allowed for smaller, faster, and cheaper computing systems, so too have we been able to improve how AI systems can enhance their learning (their predictive capability) by making predictions, observing the results of the predictions, and enhancing their probability modeling for a future time when similar observations are encountered.

There are usually many steps, or layers, to this process, depending upon the AI architecture, that are transited to arrive at a final prediction, and there are often many predictions that are used as inputs to more complex aggregators or prediction multiplexers to evaluate a real-world scenario, such as a medical image diagnosis or a self-driving car.

An ML-based AI model is created from data - lots of data. Models are created through a process called learning, or so-called "training." Different types of models examine different types or aspects of data, but essentially the model is provided with enough input data to begin to make predictions. Then the model validates its predictions against other known data and improves its understanding of the domain.

AI USES IN THE TESTING INDUSTRY

There are a number of ways in which AI is being used in the testing industry.

Test development and administration:

- *Question construction*. AI can be used in question construction; for example; by taking some instructional text and using language analysis to construct questions based on it. Such questions would usually be reviewed and adjusted by humans before use.
- *Question selection*. Some tests and exams use algorithms to select questions to present to each test-taker; for example, selecting questions for Linear on the Fly (LOFT) Testing or for Computer Adaptive Testing (CAT) or other situations where each test-taker receives a personalized assessment. AI can be used to make more effective selections.

Test scoring:

- *Written essays*. The most established use of AI in the testing industry is to automatically score essays, used to provide writing evaluation feedback and to help score exams. Systems like these have been used for such purposes since the late 1990s.
- *Audio responses*. In recent years, AI has also been used to recognize speech and to score responses in spoken English and other language proficiency exams. For example, a test-taker is asked a question and speaks the answer; the AI assigns a score or grade to the answer, based on the analyzed quality of the response.
- *Video responses*. Much more recently, AI is also used to score video recordings. For example, a job applicant can be asked to submit a video response to a series of questions; AI is used to evaluate and score the responses, and – in some cases – to screen out applicants who do not seem appropriate for the job role.

Test integrity:

- *Video analysis*. Online proctoring systems use algorithms including AI to analyze video and other data to identify behaviors that could be integrity issues (e.g., persistent looking away from the screen, having a second person assist in taking the test). Such issues are flagged, typically to human proctors or reviewers to determine if they are genuine integrity violations.
- *Biometrics analysis*. Online proctoring systems can also use AI to assist in facial recognition or other analysis of biometrics to help in identification. AI may even be used to simply recognize/match a test taker's identity at the time of a testing event with a photographic image uploaded at registration.
- *Fraud detection*. Machine learning and other AI techniques can also be used to analyze and look for patterns in data captured during testing to identify irregularities or anomalies that could be cheating or other test integrity issues. In some cases, the AI can identify a statistical rationale for the anomaly; in other cases, machine learning or other AI may identify a potential issue without being able to explain its rationale (in which case the problem will be resolved by human intervention).

Other AI use cases:

- *Data analysis*. Data analytics techniques that include AI can be used to analyze assessment data sets and make predictions or other analysis; for example, predicting job competence or needed learning or compliance risks based on assessments.
- *Individualized learning*. Educational Tech companies are increasingly using AI to aid in creating individualized learning, where machine learning and powerful data analysis can make more effective personalized learning paths, as well as to assess competence using a variety of data.

RISKS FROM AI TESTING USE CASES

One only has to perform an internet search of the term "*risks of AI*" to read the alarming predictions of the potentially harmful, and even catastrophic, dangers of a world where AI is woven throughout our daily lives. As with any users of AI, testing organizations must be certain that the technology has been designed and trained with privacy and protection of individual rights in mind. Thus, a diverse population must be accounted for by both AI researchers and scientists in the creation of the technology, as well as in the back-end training of the technology.

Speaking recently to the New York Times, a Princeton computer science professor noted, "A.I. researchers are primarily people who are male, who come from certain racial demographics, who grew up in high socioeconomic areas, primarily people without disabilities."[8] Put more succinctly, "AI is developed by humans and humans are inherently biased." When inherent bias and a diverse user population are not accounted for in developing and using AI there are great risks related to bias and discrimination in outcomes.

For testing, those might include scoring anomalies that are flagged as security and/or integrity escalations, and even learning paths that may not account for the personalized learning needs of all populations of individuals, for example individuals with disabilities. Further, where AI is utilized in conjunction with personal data, testing organizations must consider all of the legal and regulatory requirements associated with processing personal data and the risks associated with noncompliance.

While risks related to fairness, bias, and added categories of personal data collection and processing are currently most relevant to the testing industry and the use cases provided above, additional risks have been highlighted by pioneers in research and technology, such as Stephen Hawking and Elon Musk. The University of Cambridge points out several broad AI risks that may help to put the need for responsible use of AI in testing applications into perspective:

- job automation that takes away jobs from humans in lieu of automated processes, algorithms and robotics;
- physical safety risks and accidents inherent in AI-operated machines like vehicles and construction equipment;
- malicious use of AI to infiltrate digital, physical and/or political ("deepfakes") integrity and security;
- socioeconomic inequality; and, lastly,

[8] Thomas, Mike, *6 Dangerous Risks of Artificial Intelligence*, January 14, 2019; updated October 1, 2020. **https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence**

- weapons automatization.[9]

In order to understand how these issues have come into play, it is important to review the evolving ethical principles and legal/regulatory landscape prompted by public concerns about AI. A number of legal requirements have been enacted regarding use of AI – more requirements are expected in the next few years.

AI STANDARDS AND FRAMEWORK

Over the past five years numerous organizations throughout the world, including inter-governmental organizations, advocacy groups, multi-stakeholder initiatives and private companies have developed principles, frameworks, guidance, and in some instances, voluntary consensus standards, for the ethical and responsible development and use of AI ("Principles Documents").

As this White Paper is written, there are more than 60 examples of AI Principles Documents, with many others still under development. One of the most important and influential document is the "Principles on AI," published in May 2019 by the Organisation for Economic Co-operation and Development (OECD), which was adopted individually by the United States and collectively by the G20.[10] [ATP has submitted **comments** on proposed changes to AI classifications of the OECD Principles on AI.]

Other influential and representative examples of AI Principles Documents include "Ethics Guidelines for Trustworthy AI," published by the European High Level Expert Group on AI in April 2019[11] and "Microsoft AI Principles," published by Microsoft in February 2018.[12] Although all of the AI Principles Documents provide relevant, thoughtful and well-reasoned principles and guidance on the development and use of AI, few of them qualify as voluntary consensus technical standards.

[9] Id.; Callahan, Guv, *What are the Potential Risks of Artificial Intelligence?* January 5, 2021. **https://www.rev.com/blog/what-are-the-potential-risks-of-artificial-intelligence**; University of Cambridge Centre for the Study of Existential Risk, *Risks from Artificial Intelligence*. **https://www.cser.ac.uk/research/risks-from-artificial-intelligence/**;

[10] Organisation for Economic Co-operation and Development, 'Recommendation of the Council on Artificial Intelligence' (2019) p. 7 **https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449**; G20 Trade Ministers and Digital Economy Ministers, 'G20 Ministerial Statement on Trade and Digital Economy' (2019) https://www.mofa.go.jp/files/000486596.pdf.

[11] **https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai**

[12] **https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6**

Like several other pioneering areas of science and technology, the development of AI raises a host of legal, ethical, and societal issues that create real and perceived challenges for developers, policy makers, and users — including the general public. These are matters appropriate for consideration in the policy realm to be applied in the development and deployment of AI technologies and systems. Standards are one tool for implementing or informing policies and principles related to such issues.[13]

One important example of an AI standards initiative presently under way is that of the U.S. National Institute of Standards and Technology ("NIST", part of the US Department of Commerce), which is in the process of soliciting input from US federal agencies, the private sector, academia, non-governmental entities, and other stakeholders with interest in and expertise relating to AI.[14]

In addition, the Institute of Electrical and Electronics Engineers Standards Association ("IEEESA") recently launched an AI standards development initiative that may be of significant interest to testing organizations seeking guidance in this area, that includes the following standards:

- IEEE P7000™ - *Standard for Model Process for Addressing Ethical Concerns During System Design*;
- IEEE P7001™ - *Standard for Transparency of Autonomous Systems*;
- IEEE P7002™ - *Standard for Data Privacy Process*;
- IEEE P7003™ - *Standard for Algorithmic Bias Considerations*; and
- IEEE P7004™ - *Standard for Child and Student Data Governance*.

Although it will likely take several years for these standards to be completed and approved, in the meantime, testing organizations may benefit from participating in these open IEEESA standards development processes, or voluntarily following them.[15]

Given the absence of consensus technical standards for the development and use of AI systems in testing applications or even broader applicable AI consensus standards from ANSI, ISO/IEC, IEEESA or NIST testing organizations seeking guidance from the AI Principles Documents may be overwhelmed by their sheer volume and breadth and have a hard time deciding which documents to review and rely upon.

---

[13] U.S. LEADERSHIP IN AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools Prepared in response to Executive Order 13859 Submitted on August 9, 2019, National Institute of Standards and Technology of the US Department of Commerce (p. 10).
https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

[14] Id.

[15] **https://standards.ieee.org/initiatives/artificial-intelligence-systems/index.html**

Fortunately, although the AI Principles Documents vary in authorship, objectives, scope, and even the intended audience, the frameworks and individual principles developed over the past five years have coalesced around a set of common higher level principles and themes that appear to some degree in nearly all of the documents. Most AI Principles Documents are organized under the following eight high-level principles, each of which typically includes a series of sub-principles: (1) privacy; (2) accountability; (3) safety and security; (4) transparency and explainability; (5) fairness and non-discrimination; (6) human control of technology; (7) professional responsibility; and (8) promotion of human values.[16]

Common additional sub-principles under each of the high-level principles that have direct applicability to testing and assessment include:

- *Privacy*: consent, control over data use, ability to restrict data processing, right to correction, right to be forgotten, recommend additional data protection laws, and privacy by design.
- *Accountability*: verifiability and replicability, impact assessments, evaluation and auditing requirements, ability to appeal, remedy for automated decision, liability and legal responsibility.
- Safety and security: security by design and predictability.
- *Transparency and explainability*: open source data and algorithms, right to information, notification when interacting with an AI, notification when AI makes a decision about an individual, and regular reporting.
- *Fairness and non-discrimination*: bias prevention, representative and high-quality data, equality, inclusiveness in impact, and inclusiveness in design.
- *Human control of technology*: human review of automated decisions and ability to opt out of automated decisions.
- *Professional responsibility*: accuracy, responsible design, consideration of long-term effects, multi-stakeholder collaboration, and scientific integrity.

Many of the core principles and sub-principles identified in AI Principles Documents will be familiar to testing professionals because they are well aligned with existing professional standards in testing, particularly *Standards for Educational and Psychological Testing*[17] (the "Standards"), which includes standards that clearly establish the importance of fairness, non-discrimination, privacy, accuracy, human review of automated decisions and providing a right to appeal of consequential decisions in testing. Thus, the Standards continue to provide important, relevant guidance to testing organizations notwithstanding the advances in AI technology since the 2014 edition was published.

[16] Fjeld, Jessica, Nele Achten, Hannah Hilligoss, Adam Nagy, and Madhulika Srikumar. "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI." Berkman Klein Center for Internet & Society, 2020. **http://nrs.harvard.edu/urn-3:HUL.InstRepos:42160420**

[17] Standards for Educational and Psychological Testing (5th edition), American Educational Research Association, American Psychological Association, and the National Council on Measurement in Education (2014).

AI LAWS AND REGULATIONS

Currently, there are few laws that directly regulate AI, but that situation is expected to change with a continued evolution of proposed AI laws both generally and by sector. This White Paper provides only a summary of the regulatory landscape and the most prominent proposed regulations; it does not delve into an analysis of how the testing industry should comply with or respond to those regulatory efforts. However, ATP intends to monitor those regulatory activities and report on development to keep the industry apprised.

EU Proposed AI Regulation: Notably, the EU Commission recently issued proposed regulations that would heavily regulate AI systems designated as "high risk" (the "Regulation").[18] For ATP members, this Regulation as currently drafted designates as "high risk" AI systems applications that encompass individual assessment and testing. Specifically, in Annex III of the Regulation, the use of AI Systems in the following areas are designated as "high risk":

i. **Education and vocational training**:
(a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
(b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions;

ii. **Employment, workers management and access to self-employment**:
(a) AI systems intended to be used for recruitment or selection of natural persons, notably for screening or filtering applications, evaluating candidates in the course of interviews or tests…"; and

iii. **Biometric identification and categorization of natural persons**:
(a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons.[19]

The Regulation has extra-territorial reach and applies to both *users* and *providers* that place on the market or put into service AI systems, irrespective of whether those providers are established in the European Union or in a third country: *users of AI systems in the EU*; and *providers and users of AI systems that are located in a third country where the output produced by the system is used in the EU*.[20]

---

[18] ***Regulation of The European Parliament and of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts***, European Commission, 21 April 2021).

[19] ***ANNEX III*** *To The Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts*, European Commission, 21 April 2021.

[20] Id. at Title I *General Provisions*, Article 2 *Scope*

As the use of AI systems in the areas of educational, vocational training, and employment could be deemed "high risk," providers and users might be subject to a myriad of strict compliance requirements related to these uses, including implementing risk management systems, transparency and provision of detailed notice to users, post market monitoring and reporting, and conformity assessments.[21] Also notable in this draft Regulation, "high risk" AI systems must be designed in such a way as to allow for "human oversight," and a human must be able to override a system when the AI system is in use.[22]

Moreover, applicable regulators will have access to training data sets from the provider and, where necessary, the market surveillance authorities will be allowed access to the source code of the AI system.[23] This is concerning given the highly proprietary and confidential nature of the source code for AI systems. Given the tremendous impact this draft Regulation could have on ATP members, ATP intends to submit comments on the proposed Regulation, and monitor the progress of this Regulation to update members.

In addition to this draft general EU AI Regulation, there are general data protection laws, such as the European Union's ("EU") General Data Protection Regulation ("GDPR") and Brazil's General Personal Data Protection Law ("LGPD") related to automated decision making and profiling that can be applied to AI when used to process personal information.

Automated Decision-Making Laws: The GDPR regulates potentially any technology that processes personal data and was written to be technology neutral.[24] As noted by the European Data Protection Board (EDPB): "Any processing of personal data through an algorithm falls within the scope of the GDPR."[25] Thus, whenever an AI system uses personal data, all of the standard provisions of the GDPR may apply.[26]

For example, in the testing industry AI may be used during a test administration to flag irregular activities of an individual based on her/his personal information (e.g., picking up another voice or observing the test taker repetitively looking away from the camera). In testing and other situations, personal data is therefore a critical component for the full life cycle of an AI system.[27]

---

[21] *See*, Annexes V, VI, VII to the Regulation

[22] Id. at Chapter 2 *Requirements for High Risk AI Systems*; Art. 48

[23] Id at Art 64 *Access to data and documentation*

[24] Personal Data is defined in the GDPR as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (Article 4(1) of the GDPR).

[25] EDPB's **response** to EU Parliament Member, 29 Jan 2020.

[26] ***Artificial Intelligence and Data Protection: How the GDPR Regulates AI***, Centrr for Information Policy Leadership (CIPL), March 2020.

[27] Id.

Although the GDPR does not mention AI, it does mention automated decision-making. The provisions directly applicable to AI uses are Article 21 and 22. Article 21 of the GDPR gives individuals the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him or her." An organization using automated processing must provide a "clear and separate" notice of the automated process and the individual's right to object. However, the GDPR does not require the controller to disclosure its Intellectual Property Rights in making notice to data subjects.

Other countries also regulate or intend to regulate automated decision making. Brazil implemented the General Personal Data Protection Law (LGPD) in August 2020 and its data protection authority will begin enforcing it on August 1, 2021.[28] Canada is also proposing regulations of automated decision making similar to the GDPR.[29]

China's draft Personal Information Protection Law (PIPL) includes 'automated decision-making' and defines it as 'addressing personal information to be automatically analyzed and evaluated by means of computing algorithms for decision-making.' PIPL requires data processors to ensure the transparency and fairness of the decision and results and must demonstrate a legal justification for the outcome if requested by the data subject. The data subject also has the right to refuse to allow the processor to make a decision solely by automated means.[30] More countries are enacting similar laws that regulate automated decision making.[31]

In the U.S., at the state level, Virginia recently passed the Consumer Data Protection Act (CDPA)[32] that defines "profiling" as "any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location or movements." Under the CDPA, individuals in Virginia have the right to *opt out* of such profiling when it is done "in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."

---

[28] Article 20 of the LGPD includes the right to request the review and revision of solely automated decisions. *See also*, IBA - Twenty reasons why GDPR compliance does not exempt companies from adjusting to the LGPD (ibanet.org) 11 June 2020.

[29] *Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence*, March 2020 **https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pos_ai_202001/**

[30] **China: The Draft PIPL and the GDPR - A comparative perspective**, Data Guidance, Jan 2021.

[31] In Barbados, the user has the right to know, upon request to the provider, about the existence of decisions based on automated processing of personal data, including profiling; Barbados users also have the right to object to automated decision-making processes without human involvement, and to automated decisions that will produce legal or similarly significant effects on the individual, including profiling.

Panama law also grants users the right not to be subject to a decision based solely on automated processing of their personal data, without human involvement, but this right only applies when the process produces negative legal effects concerning the user or detrimentally affects the user's rights.

[32] **VACode 59.1-571 through 59.1-581, March 2021**.

Similarly, the recently enacted Colorado Privacy Act (CPA) also grants consumers the right to opt-out of profiling. The definition of profiling in the CPA closely follows that of the CDPA presented above.[33] Clearly, this language has implications for the use of automated decision-making and AI.

Testing organizations should expect more state laws and regulations related to automated decision making, so it is advisable to continue monitoring the situation in any jurisdiction where an organization operates or does business.

Video Interview Laws: Recently some states in the U.S. have passed or proposed legislation regulating the use of AI for video interviews for employment. These laws could cover testing applications when used in such instances, such as an oral test in an interview or other assessment in an employment interview. These laws generally require that notice be provided to the applicant regarding the use of AI and some require affirmative consent with the strictest seeming to be Illinois.

The Illinois *Artificial Intelligence Video Interview Act* requires employers to notify applicants when AI is used in the interview to consider the applicant's fitness for the position. Employers must provide each applicant with information before the interview about how the AI works and general types of characteristics it uses to evaluate applicants. In addition to other requirements, employers must also obtain consent from the applicant before the interview, cannot share videos unnecessarily and must delete the video upon request of the applicant.

Maryland passed a similar law (H.B. 1202) that prohibits employers from using facial recognition technology during pre-employment job interviews without the applicant's consent. Employers must obtain an applicant's written consent and a waiver that states the applicant's name, the date of the interview, that the applicant consents to the use of facial recognition during the interview and that the applicant has read the waiver.

For the testing industry, these laws may cover recorded oral examinations (e.g., language proficiency) and other evaluative types of activities during an employment interview. More states seem likely to enact laws related to AI usage for employment decisions.

Facial Recognition Technology Laws: There has been much attention given to the use of facial recognition technology in the testing industry and elsewhere. Generally, when facial recognition is used in testing for test integrity, identity verification or other uses, the technology includes AI as part of the process to verify identities of individuals or to detect anomalies about their behavior. Moreover, facial recognition technology likely includes some form of biometric capture/template and would therefore be subject to applicable laws on biometric identification and specially protected/sensitive categories of data.

[33] **CO SB 21-190 §6-1-1303(20)**.

U.S. General and Local Laws That Apply to AI: The U.S. Congress recently enacted the *National Defense Authorization Act for Fiscal Year 2021* ("NDAA"), specifically Section E.[34] This legislation is notable as it tasks the National Institute of Standards and Technology (NIST) with developing AI standards that align with international standards, as described further in the following section. It is unclear if these standards will require only federal government agencies, or private companies more broadly, to follow these standards related to the development and use of AI.

U.S. Regulatory Action and Guidance: The U.S. Federal Trade Commission("FTC") released in April 2020 a blog, *the Federal Trade Commission's Guidance, Using Artificial Intelligence and Algorithms* and included the following tips for private companies related to their use of AI: (1) Be Transparent; (2) Explain Your Decision to The Consumer; (3) Ensure That Your Decisions Are Fair; (4) Ensure That Your Data and Models are Robust and Empirically Sound; and (5) Hold Yourself Accountable for Compliance, Ethics, Fairness, and Nondiscrimination.

Although the above FTC guidance is not binding, the FTC has filed complaints against some organizations and reached substantial consent settlements related to the use of AI. One example is a $1.6M settlement with dating site AshleyMadison.com based on claims the site used fake "engager profiles" developed using AI of attractive mates to induce potential customers to sign up for the dating service.

For ATP members, the FTC enforcement demonstrates that it will pursue companies that are using AI in ways that violate the Fair Trade Act as a deceptive trade practice. State attorneys general could take action under their respective unfair and deceptive trade practice laws as well.

CONCLUSION

This White Paper has provided background information to assist the testing industry in becoming aware of and understanding what Artificial Intelligence is by reference to concepts, definition, and pervasive applications in the realm of testing and assessment. Regulation of AI is being proposed in Europe, Canada and the U.S. that may limit its future use in testing. As we learn more about the specific requirements, we plan to provide guidance in particular areas.

Because AI and its many aspects represent an extensive topic for consideration, the ATP intends to produce future bulletins of its Privacy in Practice series that will focus on specific topics such as AI in test development, AI in scoring, AI in proctoring, and AI and test integrity. Finally, given the likelihood of expanded legal requirements on the use of AI, future Privacy Bulletins could also address compliance with various laws/regulations.

[34] National Defense Authorization Act for Fiscal Year 2021, 116 H.R. 6395, 2020 H.R. 6395, 116 H.R. 6395

This document is provided "as is" and should be regarded as only general information about privacy and not as legal advice for any individual organization's specific circumstances. While there are a number of legal strategies available for the protection of personal information, each has its own strengths and weaknesses, and some are better suited than others for particular applications in testing. Moreover, although U.S. state laws exist in this area, they vary from state to state; similarly, international laws can vary significantly from country to country. Therefore, testing organizations should develop legal data protection strategies tailored to their particular circumstances and needs, and ensure that their strategies comply with all applicable laws. In order to determine the most appropriate and effective legal protection strategies to employ, testing organizations should seek the advice of legal counsel with experience representing testing organizations, especially counsel with appropriate privacy expertise.