SQUIRE PATTON BOGGS

Top Ten Things In House Counsel Should Consider About Artificial Intelligence (AI)

1. Ensure Your Legal Team and Key Stakeholders Are Educated on AI Risks and Regulation –

- **First things first: AI is already regulated.** One common misconception about AI is that it is not yet regulated. In fact, existing legal and regulatory schemes in the US and across the world regulate AI, its use, its inputs, how those inputs are or were obtained and collected, whether and to what extent the user has a legal right to use the inputs, decisions made by AI and its other outputs, the effects of those decisions and outputs, and so on. Existing privacy, intellectual property, and employment laws, just to name a few, already apply to AI.
- **More AI regulation is coming.** The forthcoming EU AI Act will apply to many companies in the US and abroad, like the paradigm-shifting GDPR. In addition, several states in the US have introduced AI-specific legislation in the last several years and new state consumer privacy laws regulate AI. The hype around generative AI has accelerated legislative activity. For information on AI-specific scrutiny from federal agencies and private litigants, see item 3 below.

2. Understand the terms of art – At its core, AI is automated processing of data, based on training data and processing prompts, that can generate outputs for specified objectives such as predictions, recommendations or objectives. There is a lot of jargon floating around out there about AI. It is therefore important to learn the key terms and make sure that your team is using common definitions when discussing AI risks and policy. A lexicon is included as an appendix. And, as the Federal Trade Commission (the FTC) warns: "AI is defined in many ways and often in broad terms … it may depend on who is defining it and for whom … what matters more is output and impact."

3. Use of AI is in regulators' and litigants' crosshairs – The FTC has signaled greater scrutiny of the use of AI is coming. A recent FTC advance notice of public rulemaking requests comment from the public on whether the FTC should ''forbid or limit the development, design, and use of automated decision-making systems that generate or otherwise facilitate outcomes that [are "unfair" or "deceptive"].'' Given the FTC's broad and fluid interpretation of what constitutes "unfair" outcomes, a business seeking to implement AI needs to carefully consider the various ways that it could impact individuals and ensure that it could defend its use. The FTC has recently blogged that "If you develop or offer a synthetic media or generative AI product, consider at the design stage and thereafter the reasonably foreseeable – and often obvious – ways it could be misused for fraud or cause other harm." The FTC is also concerned about false or exaggerated claims about the use of AI and of the capability of AI-enabled products and service. Other federal agencies are following the FTC's lead, and on April 25, 2023, the FTC issued a joint statement with the CFPB, DOJ and EEOC explaining that each agency would be using their respective enforcement authorities to regulate use of AI to protect consumers from discrimination, bias and other harms. And regulators across the world are engaging, too.

- **Canada** is considering comprehensive AI legislation: the Artificial Intelligence and Data Act, which proposes to regulate how AI is developed and used.
- **The European Union** is considering new legal frameworks, including the EU AI Act or a new Directive on AI liability. The European Union's supervisory authorities are not waiting for specific AI legislation and are already looking at AI through the lens of data protection law, launching investigations into the use of personal data to train AI, and, in some territories, have even taken action (including temporary bans in Italy) on providers of AI services.
- **Singapore's** data protection regulator has published a Model AI Governance Framework, and in conjunction with the World Economic Forum, a self-assessment guide for organizations looking to deploy AI.
- **China** issued for public comment, its draft Administrative Measures for Generative Artificial Intelligence Services on April 11, 2023, which consultation closed on May 10, 2023, and which proposed that a security assessment must be filed on services provided to the public from generative AI.
- **South Korea** is in the process of passing into law its Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI, which will identify what is classified as high risk AI for which more stringent requirements will be imposed.

Finally, private litigants are bringing cases alleging a variety of claims regarding inputs and outputs, discussed further below in item 4.

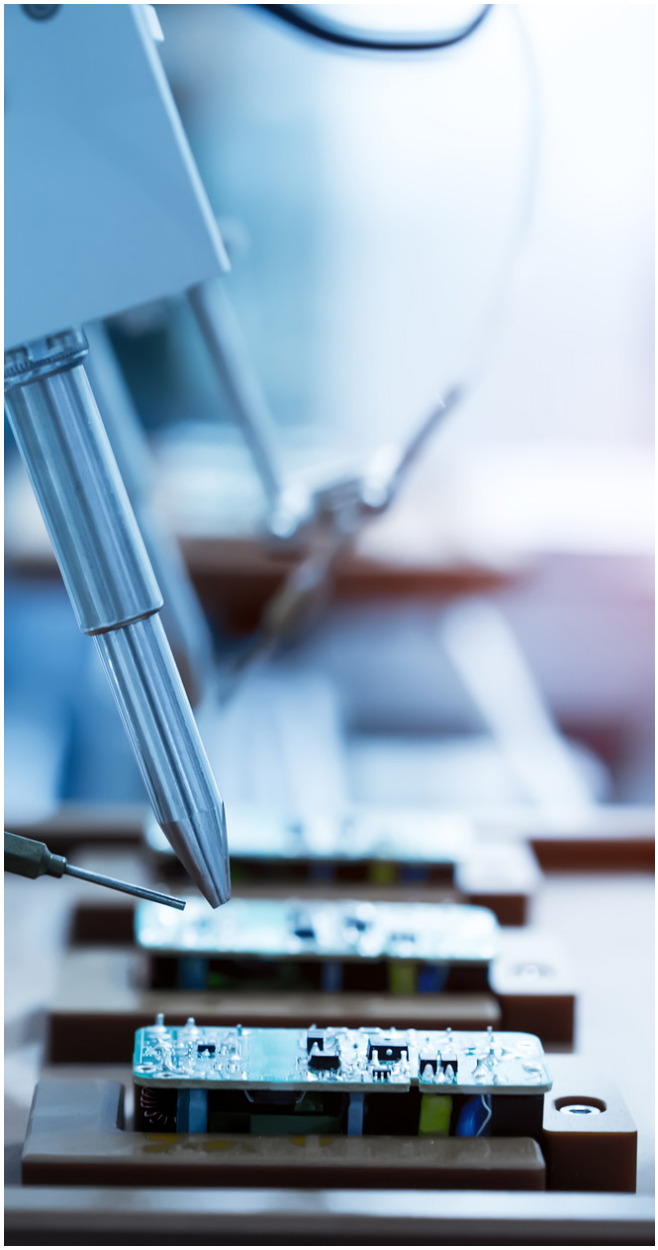
4. Develop an AI Governance Policy and Framework – A policy and a framework for applying the policy to AI development and use is crucial to ensuring legal compliance, ethical processing and risk minimization. To do so:

- Determine where you are positioned. Is your company an AI user, an AI provider, or both? This informs the potential risks and impacts, and how to address them.
- Define what AI means in your organization and your use cases. Without a clear and common definition and an understanding of how your company is using AI, it will be impossible to build an AI framework. Certainly, definitions from applicable legal frameworks should be considered. See the Appendix for a lexicon of terms.
- Leverage existing processes and procedures to address AI risks and impact: privacy and data governance, third-party risk/vendor assessments, and so on.
- Involve necessary stakeholders (e.g. IT, Security, Legal, HR, Marketing, etc.) into the process of developing and operating the company's policy and framework for development and implementation.
- Don't reinvent the wheel. Borrow and incorporate responsible AI Principles from existing frameworks, such as OECD, NIST, and ICO/IEC:
  - Ethical purpose
  - Accountability
  - Transparency
  - Fairness and non-discrimination
  - Respects privacy, confidentiality and proprietary rights
  - Complies with applicable laws
  - Safe, reliable, and secure

There is a growing body of AI governance frameworks starting from the World Economic Forum and Singapore who have published a Model AI Governance Framework and self-assessment checklist for organizations that deploy AI.

5. Conduct Risk and Impact Assessments – Internal development of AI and use of third-party AI tools should undergo an initial risk and ongoing impact assessments to identify risks of harm, the appropriateness of inputs, the credibility, non-bias and non-infringement of outputs and the effectiveness of mitigation efforts. Numerous new and proposed laws and industry frameworks call for risk and impact assessments. In addition, claims you make about AI need to be assessed as any other marketing claim.

- **Assess inputs:** AI is dependent upon training the AI with data sets to develop and improve the processing that powers AI. First, biased, stale and faulty inputs will result in output errors and other harms. Next, unauthorized use of personal data and third-party intellectual property can result in claims related to both the use of the training data to train the AI, as well as arising out of the derivatives created from its processing. Finally, unless otherwise agreed with third party AI providers, such as in a license for a private instance of the AI tool, use of company confidential and proprietary data may be used for non-company purposes, threatening trade secrets and intellectual property protections (i.e. use licensed AI that protects your inputs, rather than free public versions that do not).
- **Assess outputs:** The outputs of an AI system are essentially derivative works of the inputs, and if the inputs lacked sufficient consent to their use, the outputs can infringe third-party personal and proprietary rights. Also, there may be issues regarding the ownership of the outputs. Does the AI provider contractually take or share ownership (see item 7 below)? In the US, works not established by human authorship are not entitled to copyright protection and, thus, if the AI is generating content that might be protectible if created by a human author, the company will likely lack the exclusive rights or authorship that come with copyright if AI generates the content, which may or may not be important, depending on context. Finally, outputs may lack credibility and accuracy (e.g. AI "hallucinations," which could be libelous or otherwise harmful due to inaccuracy) and absent proper controls, can be objectionable in a variety of ways (e.g. biased, profane, or relating to illegal or undesirable activities).
- **Ensure that claims you make about your use of AI and your AI-enabled products, are accurate, not misleading, and substantiated.**



6. Speaking of Existing Laws and Regulations –

- **Privacy laws and regulations, and the regulators who enforce them, and their scrutiny on AI are here to stay.** The ban of ChatGPT by the Italian data protection authority and investigations by a handful of others have made clear that privacy and data protection should be top of mind for any and all companies implementing AI applications, particularly where personal data/personal information is implicated. The AI hype is unlikely to die down anytime soon, and, as a result, the attention by regulators likely will not either. This is amplified where processing involves more than one jurisdiction. Privacy laws are territory specific, and many of these have cross-border transfer restrictions or requirements. In Asia Pacific, for instance, several jurisdictions have data localization rules that will make AI-related processing especially tricky.
- **AI applications that are deployed in the human resources (HR) context are particularly risky in view of existing employment, privacy and other laws.**
  - In Europe, even if candidates declare their express consent for the use of AI, the employees whose characteristics are used for matching probably will be deemed not be in a position to provide freely given consent. In addition, works councils, trade unions or other employee representative committees may have co-determination rights with regard to the implementation of AI, as it may change processes in companies significantly or will enable performance or behavior control. In Germany, for instance, where works council rights are historically strong, most AI applications will require the prior signing of an agreement with the work council, and violations could lead to criminal fines.
  - California's omnibus privacy law now fully applies to California HR data as of January 1, 2023, and by this summer, the California privacy agency will issue regulations on automated decision-making and profiling that will likely have a sweeping effect on the use of AI in HR use cases.
  - New York City's law regulating use of AI in employment decisions (Local Law 144) is in effect and will be enforced by the city starting on July 5. It also provides a private right of action.
- **Intellectual Property (IP).** The overlap between AI and IP protection and enforcement is vast. Companies need to consider these issues when seeking IP protection (e.g. patents and copyrights) and also when assessing the risk of IP infringement, such as through the use of third-party data, images, content, and other materials as inputs to a generative AI system and content generated by those systems. To add complexity for global organizations, many key IP issues and concepts differ across jurisdictions.

7. Contracting related to use of AI technology is particularly thorny because of the newness of most AI technology and the rapidly evolving legal landscape – Parties on both sides must carefully consider privacy, confidentiality, data protection, data ownership and use rights, as well as the more traditional terms related to warranties, indemnities, limitations and exclusions. For example, an AI technology provider offers its AI technology "as is", reflecting the position that risk with technology innovations is a cost of doing business. The AI technology user's position is that the AI technology provider must stand behind its technology, including by providing risk and impact assessments verifying that use of the technology will not harm any individual affected by its use. Similarly, the AI tech provider asserts that data ingested by, and processed through, the technology is needed to improve the technology, whereas the technology user wants to ensure that the personal and confidential information that it submits to and through the AI technology remains private and confidential. Many AI providers offer the ability to license a private instance for a fee that allows for greater protection for the licensor, including custom controls and confidentiality of inputs and outputs.

8. Consider Cybersecurity and Incident Response – As part of the development and deployment of any AI system, IT security needs to consider how to secure any sensitive data that is used in connection with the system and how to respond in the event of a security compromise, as well as update its information security plan to address the AI system.

9. Consider Data Subject Rights – If an AI system will process personal data, one would need to consider both the lawful basis for the use of that data, as well as how data subject rights such as for access, objection to processing and deletion/erasure can be honored.

10. Treat AI Governance a Business Imperative and Compliance Imperative –

- **Business Imperative** – ChatGPT has catalyzed the discussion around, and adoption of, AI. This has your C-suite buzzing. AI governance will enable you to avoid becoming a stop sign.
- **Compliance Imperative** – Effective AI governance will assist your organization in complying with existing laws, and will be necessary to comply with existing and forthcoming AI-specific regulation such as the AI Act. If your company is an AI provider, in the next two to three years, there almost certainly will be laws requiring not only your organization's AI governance and compliance, but also to enable and assist with your customers' compliance. If your company is an AI consumer, it will still face legal limitations, obligations and risks, as well as reputational risk if prudent decisions are not made to ensure that the benefits far outweigh the risk of harms.

Key Takeaways:

- Understand the context/use case involving AI:
  - Public, third party, or internal use
  - End user interaction with AI? If so, who is the end user (employee, B2B customer, consumer, etc.)
  - Developed internally or acquired from a third party
  - How are risk (before use) and impact (during use) being assessed, and by whom
- Understand the inputs and outputs and how the processing works:
  - How are third party rights affected
  - How are the company's rights affected
- Understand what laws apply and ensure compliance.
- Determine what notices need to be provided to whom and when consents are required or prudent.
- Document assessments that establish that the AI system is used in a manner such that benefits outweigh potential harms.

Appendix

The term "artificial intelligence" or "AI" has evolved as a catch-all term for a continuum of technology by which algorithms use inputs to produce outputs. On one end of the continuum is task-specific automated processing that can handle large amounts of data to complete a task infinitely faster than a human could complete the same task. On the other end is so-called artificial general intelligence (AGI), which is a man-made intelligence that is indistinguishable from the human mind.

Most experts agree that AGI is still out of reach – and perhaps not achievable at all – but, between the task-specific algorithms and AGI are increasingly powerful AI systems trained to draw inferences from massive data in order to achieve particular outcomes. This acceleration in algorithmic sophistication – made possible by the decreased cost and increased power of cloud computing – may explain why experts have not yet settled on a consensus definition for AI.

Following are some commonly used terms that help explain this technology continuum.

What is	
AI Hallucination	"… [AI] models generate incorrect outputs but articulate them convincingly." – *OECD.AI Policy Observatory*
Algorithm	A clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result. – NIST
Algorithmic Discrimination	When automated systems contribute to unjustified different treatment or impacts disfavoring people based on their race, color, ethnicity, sex … religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law. Depending on the specific circumstances, such algorithmic discrimination may violate legal protections. – Blueprint for an AI Bill of Rights
Anonymization	A process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party – ISO/IEC 29100:2011(en)
Artificial Intelligence System	" … means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations, or decisions influencing physical or virtual environments," reads the text, seen by EURACTIV …" (March 3, 2023) "An AI system is a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g. with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy." – OECD

What is	
Automated Decision-Making*	"[T]he process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data . . . [ADM] often involves profiling, but it does not have to." – UK Information Commissioner's Office
Deep Fake	". . . believable, realistic videos, pictures, audio, and text of events which never happened" created using artificial intelligence/machine learning – US Department of Homeland Security
General Purpose AI	"AI system that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of tasks." – European Parliament
Generative AI	". . . create[s] new content in response to prompts based on their training data." – OECD "[C]olloquial term] used to refer to chatbots developed from large language models and to technology that simulates human activity, such as software that creates deepfake videos and voice clones." – US Federal Trade Commission
Large Language Models (LLMs)	A class of generative AI tools, trained on vast amounts of data, to enable content development and problem solving upon request using natural language or to write a response as a human would, with great speed. However, inherent with the nature of the training data the output can be incorrect or biased, sometimes referred to as AI hallucinations. Also, LLMs that lack good controls can be used in inappropriate ways and generate output that is undesirable, such as counsel on illegal activities and objectional or bigoted responses. Private instances of LLMs can add additional company mandated controls beyond what the developers have programmed for public versions.
Machine Learning	. . . process using algorithms rather than procedural coding that enables learning from existing data in order to predict future outcomes" – ISO/IEC 35505 Part 1: Application of ISO/IEC 38500 to the governance of data "[A] branch of computational statistics that focuses on designing algorithms that can automatically and iteratively build analytical models from new data without explicitly programming the solution." – US-EU Trade and Technology Council Inaugural Joint Statement
OECD	Organisation for Economic Cooperation and Development
Profiling	"[A]ny form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements." – General Data Protection Regulation, Art. 4(4)* "'Profiling' means any form of automated processing of personal information, as further defined by regulations [yet to be promulgated], to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." – California Consumer Privacy Act as amended by the California Privacy Rights Act
Training Dataset	"A training dataset is used to teach [AI] models to yield the desired output and includes inputs and outputs that are correctly categorized or 'labeled,' which allow the [AI] model to learn over time." – US General Services Administration

For more information on AI and how to develop and implement an ethical AI policy and framework for your business, contact the authors:

APAC

Singapore

Charmian Aw
E charmian.aw@squirepb.com

China

Lindsay Zhu
E lindsay.zhu@squirepb.com

Hong Kong

Nick Chan
E nick.chan@squirepb.com

Japan

Scott Warren
E scott.warren@squirepb.com

EMEA

UK

David Naylor
E david.naylor@squirepb.com

Belgium, France and Italy

Charles Helleputte
E charles.helleputte@squirepb.com

Diletta De Cicco
E diletta.decicco@squirepb.com

Germany

Dr. Annette Demmel
E annette.demmel@squirepb.com

Spain

Bartolomé Martín
E bartolome.martin@squirepb.com

United States

Alan L. Friel
E alan.friel@squirepb.com

Julia B. Jacobson
E julia.jacobson@squirepb.com

Kyle R. Fath
E kyle.fath@squirepb.com

Glenn A. Brown
E glenn.brown@squirepb.com