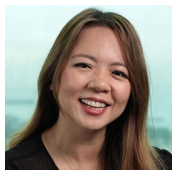


Artificial Intelligence Webinar Series

# Top Ten Things In House Counsel Should Consider About AI

May 24, 2023

# Speakers



**Charmian Aw**

Partner, Singapore  
T +65 6922 8679  
charmian.aw@squirepb.com



**Sara Belotti**

Partner, Milan  
T +39 02 7274 2001  
sara.belotti@squirepb.com



**Kristin L. Bryan**

Partner, New York and Cleveland  
T +1 216 479 8070  
kristin.bryan@squirepb.com



**David S. Elkins**

Partner, Palo Alto  
T +1 650 843 3378  
david.elkins@squirepb.com



**Kyle R. Fath**

Partner, Los Angeles  
T +1 213 689 6582  
kyle.fath@squirepb.com



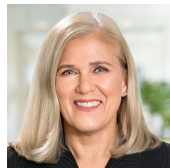
**Alan L. Friel**

Partner, Los Angeles  
T +1 213 689 6518  
alan.friel@squirepb.com



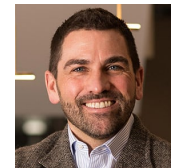
**Charles Helleputte**

Partner, Brussels  
T +32 2 627 11 00  
charles.helleputte@squirepb.com



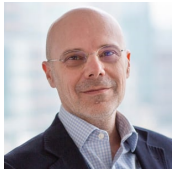
**Julia B. Jacobson**

Partner, New York  
T +1 212 872 9832  
julia.jacobson@squirepb.com



**Wolfgang A. Maschek**

Partner, Brussels  
T +322 627 11 04  
wolfgang.maschek@squirepb.com



**David Naylor**

Partner, London  
T +44 20 7655 1668  
david.naylor@squirepb.com



**Stacy A. Swanson**

Public Policy Advisor, Washington DC  
T +1 202 457 5627  
stacy.swanson@squirepb.com

# What We'll Cover

AI is already regulated and legislative momentum and regulatory activity are rapidly increasing

Develop an AI governance policy and framework and mitigate potential harms

Contracting for AI effectively and ensuring lawful use of inputs and outputs

Know that the use of AI is in regulators' and litigants' crosshairs

Treat AI governance as not just a compliance imperative but also a business imperative





AI is already regulated and legislative momentum and regulatory activity are rapidly increasing

Julia Jacobson and Wolfgang Maschek

# What is Artificial Intelligence?

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.**



Organisation for Economic Cooperation and Development (OECD)

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.**



NIST AI Risk Management Framework

AI is defined in many ways and often in broad terms ... it may depend on who is defining it for whom, and who has the power to do so ... **what matters more is output and impact.**



Federal Trade Commission (June 2022)

An engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of **human-defined objectives.**



ISO/IEC 22989:2022 (en)

- **The Economist:** OpenAI CEO S. Altman called for tighter regulation of rapidly developing generative AI “*if this technology goes wrong, it can go quite wrong*”
- **AI already regulated** to an extent, and regulatory momentum in full swing
- **New EU AI Act** in advanced discussion between the EU Parliament and the 27 EU Member States. Broad-scale regulation of AI use cases touching EU market/citizens. Adoption likely in 2023. Risk based approach, with rigid compliance rules applied *ex-ante* and extraterritorial effects (akin to GDPR)
  - Unacceptable risk: banned. E.g.: social scoring, exploitation of vulnerable groups
  - High Risk: risk management; obtain conformity assessment before market placement
  - Limited Risk: transparency requirements ...”**Brussels effect**” in action?
- **United Kingdom (UK):** lighter approach, emphasis on spurring innovation
- **China:** adopted AI rules re algorithms and online user recommendations

## Laws


- Canada – AI and Data Act (AIDA) (*under consideration*)
- U.S. – NYC Local Law Int. No 1894-A (2021) and Implementing Rules (2023)
- Consumer Protection Laws
- IP Laws
- Privacy/Security Laws

## Voluntary Frameworks

- OECD Framework for Classification of AI Systems (Feb 2022) and OECD AI Principles (May 2019)
- ISO/IEC 23054: 2022 Framework for AI Systems Using Machine Learning
- U.S. – NIST Risk Management Framework 1.0 (Jan 2023); White House “AI Bill of Rights” (Oct 2022)
- Singapore – A.I. Verify (voluntary AI Governance testing framework)

## Regulatory Guidance

- UK Government White Paper on “A Pro-Innovation Approach and to AI Regulation” (March 29, 2023)
- U.S. EEOC Technical Assistance re Americans with Disabilities Act and the use of AI to assess job applicants and employees (May 21, 2022)
- Federal Trade Commission (various – 2020-2023)



# Develop an AI governance policy and framework and mitigate potential harms

David Naylor and Stacy Swanson



# Develop an AI governance policy and framework and mitigate potential harms

## The key elements of an effective AI governance framework

- Capture all proposed acquisition and development of AI across the business
- Identify proposed uses that would be potentially unlawful or highly regulated **early**
- Horizon-scanning is **critical**




# Develop an AI governance policy and framework and mitigate potential harms

## The key elements of an effective AI governance framework

- Weed out proposals for potentially unlawful systems
- Identify ADM that's likely to have a legal or similar effect
- Ensure training data has been lawfully acquired **and** can be lawfully used
- Conduct impact assessments and implement risk mitigation regimes
- Diligence third party AI services and data providers and ensure compliant terms in place
- QA outputs
- Keep horizon scanning!
- **Senior management buy-in is critical**





Contracting for AI  
effectively and  
ensuring lawful use of  
inputs and outputs

David Elkins and Kyle Fath

# Third-party risk: Contracting effectively and ensuring lawful use of inputs and outputs

- Verifying that a company complies with applicable regulations regarding the use of artificial intelligence is increasingly an extremely important part of due diligence processes.
  - Products /services compliance (i.e., compliance with regulations in relation to what a company offers to the market and against which the company generates its revenues); and
  - Internal corporate compliance (i.e., compliance with regulations in relation to internal AI-related tools used by the company to run its business).
- Noncompliance is a (negative) figure, and it is an amount that is discounted from the value of your company
  - Estimated costs needed to be compliant in the future; and
  - Risks associated with non-compliance in the past.
- Routinely monitoring your company's compliance is a matter of continuous learning and a precious value to all stakeholders.


## Know what the landmines are and where they lay



- The potential landmines of AI inputs and outputs and the consequences of ignoring them
- How to reduce IP, privacy, and other legal risk by:
  - Anticipating the landmines
  - Tailoring commercial agreements, taking into account whether you are an AI developer/provider, incorporating third-party AI tech, or an AI end user

## Maximize protection through third-party assessments and addressing risks in commercial agreements

- Source of training data?
- Ongoing rights to your inputs
- Responsibility for/enabling/assisting with compliance
  - Historical and ongoing testing for bias/discrimination, accuracy/reliability, lawfulness, etc.
  - Features for transparency/explainability to end users
  - Ability to insert human review/input into any decision-making processes
  - Honoring privacy choices
- Representations and warranties, liability shifting (indemnification), etc.



Know that the use of AI  
is in regulators' and  
litigants' crosshairs

Charles Helleputte and Kristin Bryan


# Know that the use of AI is in regulators' and litigants' crosshairs

- The (upcoming) EU AI Act provides for decentralized enforcement (i.e., at Member States level). Data protection authorities should be at the helm
  - So, GDPR-type enforcement (and GDPR-type fines) *versus* central enforcement (such as in the DSA). Main questions? Central role but this assumes DPAs get the necessary resources (e.g., the AI Act has cybersecurity (and robustness) as one of its core pillar, will there be enough skilled firepower?). What about unharmonized enforcement agenda?
- **BUT** there is more than the EU AI Act. In the European Union alone, AI, as a technology, and AI uses in particular are getting a lot of attraction from regulators and courts (and this is not new)
  - Sector-specific, e.g., work done by ESMA, EBA and EIOPA in the financial sector (“wait & see”) or sector-agnostic, e.g., by the EU itself (EU Center for Algorithmic Transparency, as part of DSA)
  - Enforcement by data protection authorities (e.g., Garante and CNIL actions in relation to OpenAI)
  - Far-reaching calls for accuracy and transparency in an ADM cases, e.g., Slovak Constitutional Court (and similar call in the Foodinho case from the Italian DPA)
  - AI liabilities might lead to collective redress incentives (but patchwork of legal cultures)



# Know that the use of AI is in regulators' and litigants' crosshairs in the U.S. as well

- AI is also an area of focus in the U.S., with a rise in federal regulatory scrutiny and litigation brought by plaintiffs in putative class actions.
- This month the Federal Trade Commission (FTC) warned that the increasing use of technologies powered by machine learning raises significant privacy and security concerns and implicates the potential for bias and discrimination.
- Other areas of focus include novel uses of AI that could potentially deceive consumers and the FTC's use of algorithmic disgorgement as a penalty in enforcement actions.
- Additionally seeing a rise in civil litigation related to use of AI, with recent virtual-try on claims against cosmetics companies and eyewear retailers as one such example and more AI based claims anticipated in future. Could include in relation to data security issues and deceptive marketing claims, among others.

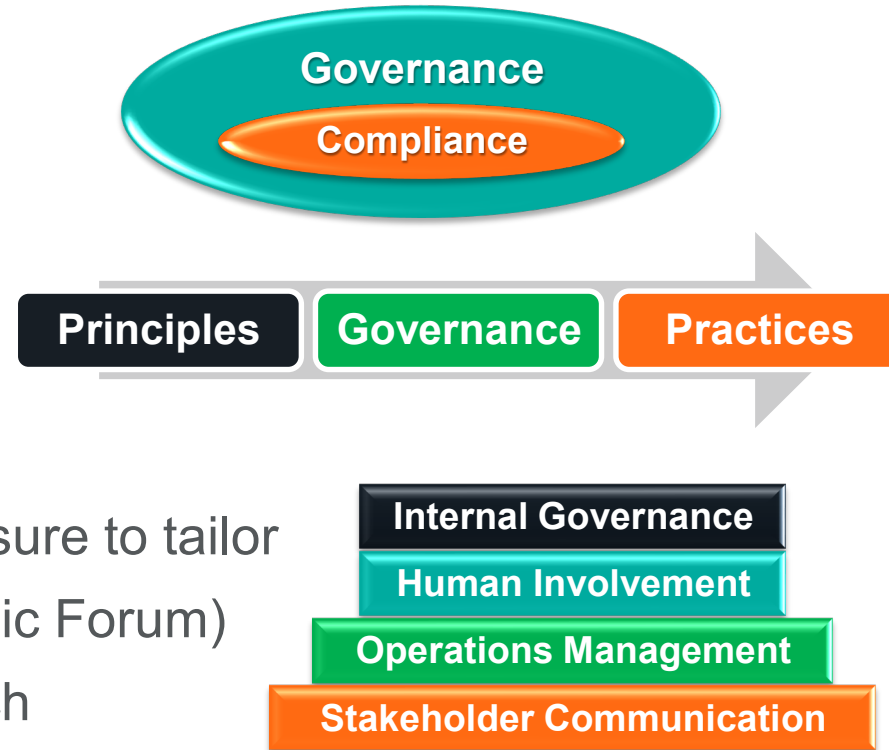


Treat AI governance as  
not just a compliance  
imperative but also a  
business imperative

Charmian Aw and Sara Belotti

# Treat AI governance as both a business imperative and a compliance imperative

- How is governance a value-driver?
  - Facilitates compliance
  - Mitigates risk
  - It also goes beyond
- How to construct?
  - Don't reinvent the wheel – but be sure to tailor
  - Model Framework (World Economic Forum)
  - Work with experts with global reach



# Treat AI governance as both a business imperative and a compliance imperative

- Verifying that a company complies with applicable regulations regarding the use of artificial intelligence is increasingly an extremely important part of due diligence processes.
  - Products /services compliance (i.e., compliance with regulations in relation to what a company offers to the market and against which the company generates its revenues); and
  - Internal corporate compliance (i.e., compliance with regulations in relation to internal AI-related tools used by the company to run its business).
- Noncompliance is a (negative) figure, and it is an amount that is discounted from the value of your company
  - Estimated costs needed to be compliant in the future; and
  - Risks associated with non-compliance in the past.
- Routinely monitoring your company's compliance is a matter of continuous learning and a precious value to all stakeholders.

- **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.**

For those of you who require CLE credits please note the following states are approved for 1.0 general hour of CLE (AZ, CA, CT, NJ, NY and OH (pending)).

Lawyers who have CPD requirements in England & Wales and Ireland may use the CLE certificate as proof of attendance.

Please write down the following affirmation code: **AI524**

After today's session you will receive a Uniform Certificate of Attendance to submit to [robin.hallagan@squirepb.com](mailto:robin.hallagan@squirepb.com). Please add the code and your attendance will be added to the CLE tracker.

# Speakers



**Charmian Aw**

Partner, Singapore  
T +65 6922 8679  
charmian.aw@squirepb.com



**Sara Belotti**

Partner, Milan  
T +39 02 7274 2001  
sara.belotti@squirepb.com



**Kristin L. Bryan**

Partner, New York and Cleveland  
T +1 216 479 8070  
kristin.bryan@squirepb.com



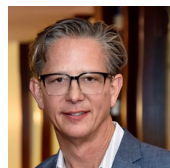
**David S. Elkins**

Partner, Palo Alto  
T +1 650 843 3378  
david.elkins@squirepb.com



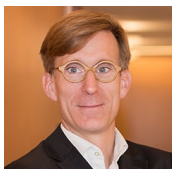
**Kyle R. Fath**

Partner, Los Angeles  
T +1 213 689 6582  
kyle.fath@squirepb.com



**Alan L. Friel**

Partner, Los Angeles  
T +1 213 689 6518  
alan.friel@squirepb.com



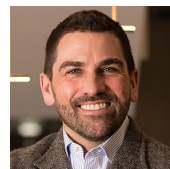
**Charles Helleputte**

Partner, Brussels  
T +32 2 627 11 00  
charles.helleputte@squirepb.com



**Julia B. Jacobson**

Partner, New York  
T +1 212 872 9832  
julia.jacobson@squirepb.com



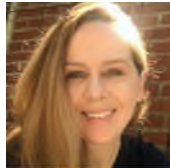
**Wolfgang A. Maschek**

Partner, Brussels  
T +322 627 11 04  
wolfgang.maschek@squirepb.com



**David Naylor**

Partner, London  
T +44 20 7655 1668  
david.naylor@squirepb.com



**Stacy A. Swanson**

Public Policy Advisor, Washington DC  
T +1 202 457 5627  
stacy.swanson@squirepb.com

## Global Coverage

Abu Dhabi  
Atlanta  
Beijing  
Berlin  
Birmingham  
Böblingen  
Bratislava  
Brussels  
Cincinnati  
Cleveland  
Columbus


Dallas  
Darwin  
Denver  
Dubai  
Dublin  
Frankfurt  
Hong Kong  
Houston  
Leeds  
London  
Los Angeles

Madrid  
Manchester  
Miami  
Milan  
New Jersey  
New York  
Palo Alto  
Paris  
Perth  
Phoenix  
Prague

San Francisco  
Santo Domingo  
Shanghai  
Singapore  
Sydney  
Tampa  
Tokyo  
Warsaw  
Washington DC

Africa  
Brazil  
Caribbean/Central America  
India  
Israel  
Mexico

 Office locations

 Regional desks and strategic alliances

