State of AI Regulation

The EU, UK, China and the US all have existing regulations that cover the development and deployment of AI. Of these, the Chinese rules are presently the most developed.

The EU has drafted a new regulation that is expected to be in force from 2025; this law will introduce very substantial additional requirements for the use of AI along with considerable additional financial and other penalties. The US has a number of initiatives including a proposed federal "AI bill of rights" along with FTC consultation, a proposed regulatory framework from the National Institute of Standards and Technology and a continually developing body of state law.

The UK has recently published a white paper setting out its proposed approach to AI regulation, which is self-described as "pro-innovation" and might reasonably be considered to be lighter-touch than the other existing and forthcoming regulations considered here. The core purposes of all of these present and future regulations can be summarised as seeking to ensure transparency, fairness, safety and recourse.

EU

- GDPR article 22 plus local laws
- EU AI Act (coming 2025)
- Digital Services and Digital Markets Act

US

- US AI executive order 14110
- Whitehouse Blueprint for AI Bill of Rights
- NIST AI Risk Management Framework
- FTC and employment enforcement
- State laws

China

- AI Ethics code
- PIPL
- Watermarking for AI imagery

Others

- Singapore (model AI governance framework)
- UK (white paper)
- OECD framework
- Brazil

Types of AI

The terms AI and machine learning cover a wide range of systems. Existing and future regulation takes a wide view, meaning that it covers not only "cutting edge" tools—such as ChatGPT or StableDiffusion—but also much more conventional decision-support systems including basic fixed decision logic and so-called "expert systems", which generally operate to defined rules rather than being based on learning from large datasets. This in turn brings much of a business's IT estate into scope.

- Generative models (LLMs, visual engines, audio)
- Machine vision, physical autonomy and contextual response (robots, cars, drones etc)
- Case specific machine learning (scientific exploratory, Alpha Go, medical diagnostics)
- Deterministic decision-making and decision-support systems (expert systems)
- …and any other algorithmic decision-and any other algorithmic decision-making *of any kind*

Three Pillars of Governance

Inputs

Bias
Right to use
Revocability
Data rights
Representation
Feedback loops
GIGO

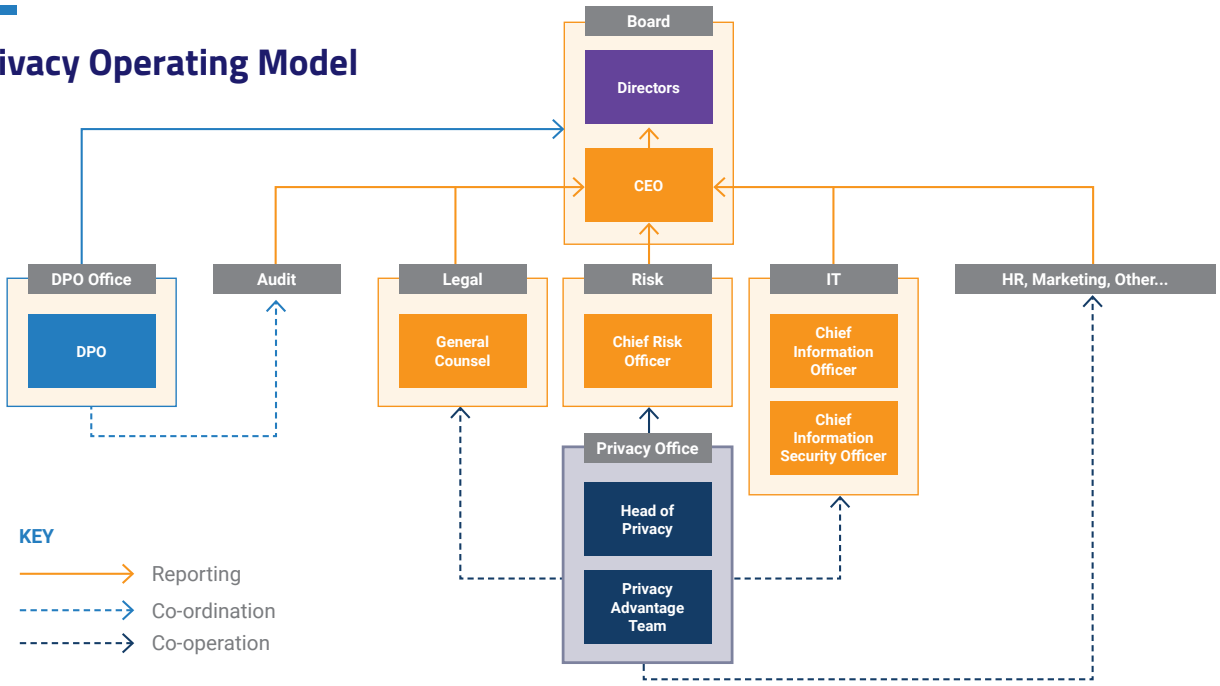
Decisions

Bias
Transparency
Reproducibility
Correlative error
Hallucination
Hinting
Intervention
Governance
Appeal

Consequences

Bias
Disadvantage
Reputational risk
Error reinforcement
Loss of IQ/EQ
Recombination
Leakage
Abuse

Privacy Operating Model



For more information

Ben Rapp
Founder & Principal
—
ben.rapp@securys.co.uk

James Flint
Senior Consultant
—
james.flint@securys.co.uk