SQUIRE PATTON BOGGS

Reconciling Artificial Intelligence (AI) With Product Safety Laws

A High Stakes Challenge for the 2020s

Europe – December 2023

Introduction

We are at the start of an AI revolution, and thoughts have started to turn from science fiction to reality – in particular, whether the possible advantages that AI could bring outweigh the risks.

One area of concern is that the use of AI, or products that AI are used in or with, could present risks to human health and safety; for example, in the event of inherent or latent defects in software, or if systems are "hacked". Current "general" product safety laws that apply in many countries around the world could cover some aspects of the potential risks, but not all, and not with any specificity.

Governments in numerous countries are grappling to understand how product safety regulation can keep pace with technological advances and balance risk against reward. The UK, for example, wishes to be an AI "superpower", but can it navigate the challenges of developing product safety laws to adequately cover the risks it presents?

Background

AI, or the "modelling of human mental functions by computer programs", is Collins Dictionary's Word of the Year for 2023. This is no surprise, as the promise of simplicity, clarity and efficiency for users and products is an attractive one. However, these ambitions risk instead slipping into complexity, opacity and cost for businesses if governments do not act to regulate the challenges posed by the proliferation of AI technologies, or at least do not regulate them in the right way.

It has been said many times that AI will "disrupt" most industries, and it seems the knock-on effect on product safety considerations is inevitable. However, existing EU and UK product safety laws, which have served as examples worldwide, were not designed to accommodate technologies that were unknown when the legislation was conceived.

As AI becomes more commonly integrated into consumer products, reform is needed to protect people and provide businesses with certainty on the extent of their obligations, and a framework within which to operate. The nature of AI as a mutating, data-reliant and autonomous technology is an inherent challenge to any sort of predictability around enforcement mechanisms, mitigation of harm, and where responsibility for safety should sit. While these same issues face all governments, each jurisdiction will likely approach them in their own way, perhaps dependent on other priorities, including fostering economic growth.

Therefore, businesses will also have to grapple with regulatory divergence, even across Europe, as the EU and the UK's product safety regimes will almost certainly differ post-Brexit, albeit with some commonalities.

Discussions at the AI Safety Summit, held at the beginning of November in Bletchley Park, brought together leading AI companies, governments and researchers. The Center for Democracy & Technology notably called for governments to "prioritise regulation to address the full range of risks that AI systems can raise, including current risks already impacting the public".

Beyond policy, meetings and speeches, legislative change is fast approaching. Last month, the EU announced it was "within touching distance" of agreeing unprecedented laws to regulate AI across its member states. The EU is leading the charge on regulating AI, attempting to reconcile it with key legal concepts of liability, ownership and negligence – the UK, meanwhile, is currently keeping its cards closer to its chest. The UK government and the "pro-Brexit" lobby have commonly cited Brexit as an opportunity to limit red tape to allow innovation and growth, although the holding of the AI Safety Summit in Bletchley is perhaps an indication that the UK government is wrestling with how to balance flexibility to innovate with protection from possible risks to human health and safety.

Meaning of AI and Relevance to Product Safety

Regulators and commentators have penned their own conceptions and definitions of AI. In the EU Commission's 2018 communication Artificial Intelligence for Europe, it was described as "systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."

"AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)."

In a similar vein, the UK Office for Product Safety and Standards, in a December 2021 Report (OPSS Report), described AI as "a broad term referring to computer systems that can sense their environment, think, possibly learn and take action in response to what they are sensing or their objectives."

AI systems have already been adopted across different aspects of the lifecycle of other products intended for consumers or likely to be used by consumers or workers. For example, AI is emerging as a way to decrease mining accidents through "smart caps" to analyse the brainwaves of vehicle drivers and issue an alert when drowsiness and fatigue are detected. However, one industry concern is that adding AI into existing products will change the product's functioning during its lifecycle and could create risks that did not exist at the point that the product was placed on the market and assessed as safe.

In addition, there are reports that AI is being used in automated manufacturing (for example, humanoid robots for Amazon)[1]; predictive maintenance (using sensors to monitor the condition of equipment, such as that reported to be used by Colgate-Palmolive Company); and quality control (automation and analysis of historic data to identify defects in the quality process).

The OPSS Report highlights the opportunities and challenges of incorporating AI systems into manufactured consumer products. It highlights safety benefits for consumers due to its ability to enhance data collection processes during industrial assembly of consumer products to help prevent mass product recalls and to allow engineers to input information on restrictions, production methods, material and other variables into an algorithm that can reduce human time and effort. It also highlights the possibility of greater customisation and personalisation, with consumer preferences taken into account during the design process, perhaps directly from the consumer's own voice.

The (largely theoretical) risks highlighted include a number related to product safety, which centre around the idea of an AI-driven system malfunctioning as a result of automated decisions and causing physical injury. The risks are related to:

- **The characteristics of AI as a technology** – Including mutability, opacity, data needs and autonomy, all of which can translate into errors or challenges for AI systems that have the potential to cause harm.
- **Robustness and predictability** – Poor decisions or errors made in the development phase of an AI project and insufficient or poor-quality data can lead to poor algorithmic performance.
- **Transparency and explainability** – Which can impact the consumer's understanding of responsibility for a defect or other safety issue, or what action should be taken to remedy an issue.
- **Security and resilience** – Cybersecurity vulnerabilities in consumer products that may enable consumer harm (the OPSS Report cites a real-world product recall of smartwatches for children that allowed access to sensitive personal data, such as location history, phone numbers and location tracking).
- **Various immaterial harms** – As a result of fairness and discrimination, impact on vulnerable groups, and privacy and data protection challenges. The example given in the OPSS Report is the gradual replacement of human contact for older people with autonomous products causing mental health issues.

Coverage of AI Risks Under Current Product Safety Laws?

Safe products are generally understood, under current product safety laws at an EU and UK level, as products that, under normal or reasonably foreseeable conditions of use, do not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons.

1 Subscription required

It is easy to see how the incorporation of AI into consumer products (or "hardware") could affect safety in this context. A glitch in the software, an error in the data received, or a cyber-attack, could cause a product's malfunction, or use by a consumer in an unsafe way, or could result in a failure to indicate that safety-critical maintenance of the product is required. Inaccurate or incomplete instructions on how to use the AI within the product could also mean that it is used in an unsafe way, or perhaps if the AI within the product is itself used to provide instructions and warnings for use of the hardware, a glitch could mean that an otherwise safe product, if used as intended, could become unsafe, because of a lack of, or inaccurate, warnings.

Where AI is used for predictive maintenance of equipment used to produce consumer products, or to assist with quality control procedures, a defect or fault in the AI, either immediately or during the lifetime of the AI or the product, could also affect product safety, for example, because it could result in a product not being manufactured consistently in accordance with a safe design or specification. Where AI is used in automated manufacturing, the same issue could arise. Of course, this is not dissimilar to risks with software that has been used for predictive maintenance in manufacturing contexts for several years, if the software has not been programmed or updated correctly. However, the difference with AI is that the system is "learning as it goes", so it could be much more difficult to determine if the glitch is as a result of the initial programming or updates (or lack of them), or for some other reason that has impacted the way that the system has "learned".

Current EU and UK product safety laws prescribe that in determining whether a product is a safe product, a number of factors are taken into account, including instructions for installation and maintenance, warnings, instructions for use, and the effect of a product on other products, where it is reasonably foreseeable that it will be used with other products. Therefore, it is likely that these current laws could operate to some extent to regulate AI if it is accepted that current definitions of "product" are wide enough to encompass computer systems and software used in or with "hardware" products.

However, this is of course only an interpretation, and an application of laws that were never designed to regulate AI specifically and which, in fact, predate widespread use of such technology. As such, they do not operate in a way that provides a clear framework for the design and development of AI for the benefit of businesses and regulators, and they certainly do not provide clarity over potential responsibilities where a complex chain of parties could be involved in getting an AI product – or a product that contains or is used with AI – to market, or installing or maintaining it, or providing instructions for its use.

For example, where AI is incorporated in a car, parties could include (as a minimum) the software designer(s), the software developer(s), an engineering team that incorporates the software into the car, a team that provides the information fed into the software (for example, instructions for use of the vehicle), the car designer, the car manufacturer, and the garage that carries out maintenance and servicing of the car, including potentially its computer systems.

It is foreseeable that an error or oversight by any of these economic operators along the supply chain related to the development of the AI, or its use with the car, could result in a safety issue, and that would be a very tangled web to untangle!

Will AI Be Regulated Differently to Other Products in Future?

Twenty-five countries have now backed the Bletchley Declaration, which focuses on identifying risks and building cross-border policies to minimise them. In his own statement on 2 November, Prime Minister Rishi Sunak said, "Until now, the only people testing the safety of new AI models… have been the very companies developing it. That must change."

This will, no doubt, catch the attention of product safety professionals, as "self-certifying" that a product meets a particular standard is precisely how many current product safety regimes in the EU and the UK operate, with the exception of typically higher-risk products that involve testing and certification by notified bodies, which are generally instructed by the companies developing the product, or its "manufacturer". Requirements for toys, medical devices, machinery, electrical equipment and personal protective equipment (and others) all follow this model, whereby certain lower risk "classes" of each product are declared to conform with essential safety requirements by the manufacturer itself, before a CE mark or UKCA mark is applied to the product, as a visual indication of the conformity assessment process being carried out by the manufacturer. Even where a notified body is required for conformity assessment or approval of a quality system of those higher risk "classes" of product, the manufacturer is responsible for drawing up the technical documentation and product conformity.

However, the difference with those other product compliance regimes is that conformity can usually be assessed by reference to harmonised or designated standards, or other prescriptive technical specifications for certain product types, which are intended to ensure that essential safety requirements are met. It is difficult to see how there could be a set of detailed standards or specifications that would allow such rapidly moving technology to be assessed independently, at least while the "AI revolution" is in its infancy, because each possible "product-type" or use of AI is as yet unknown and untested. Therefore, it is certainly possible that the regulation of AI will not follow the model for other product types and, as such, it seems likely that a new model may need to be developed in future.

Reforms – Recent Developments and Proposals

Developments in the EU

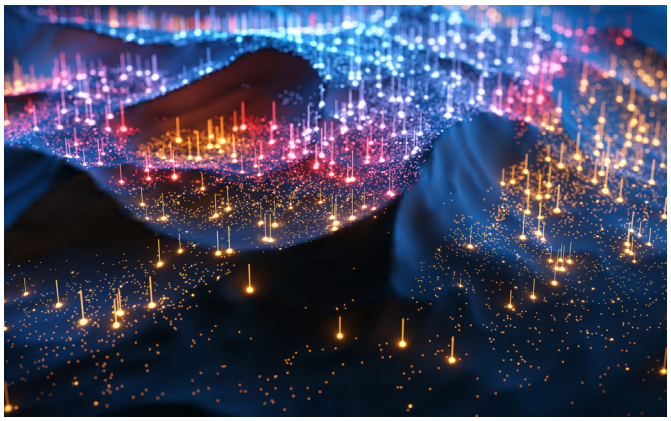
The EU Parliament has been clear that its priority is that AI systems in the EU be safe, transparent, traceable, non-discriminatory and environmentally friendly. The upcoming measures are:

- A new General Product Safety Regulation for the EU (GPSR) to replace the existing General Product Safety Directive (2001/95/EC) (GPSD).

  The GPSR entered into force on 12 June 2023 and will apply in the EU from 14 December 2024. As with the GPSD, the new GPSR will apply to products that are not already subject to product-specific regulations (for example, regulations that apply to toys, electronic equipment, lifts, medical devices and foods). It contains a similar overarching definition of what a "safe product" is to the definition in GPSD. As set out above in relation to the existing regime, this is likely broad enough to ensure that if AI poses a risk to human health or safety, it can be enforced by reference to GPSR. Although GPSR does not contain specific provisions referring to AI, it expands the current regime to cover new technologies and online marketplaces (like Amazon and eBay). It also "adds" to the list of what will be taken into account in assessing the safety of products. The following factors are of particular relevance to AI:

  - When required by the nature of the product, the appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, where such an influence might have an impact on the safety of the product, including the possible loss of interconnection
  - When required by the nature of the product, the evolving, learning and predictive functionalities of the product

  As an EU regulation, the new GPSR will apply directly in all EU member states, but it will not apply in the UK because it is being implemented post-Brexit.



- New AI-specific regimes in the form of an AI Act and an AI Liability Directive.

  The AI Act is intended to regulate the providers that place on the market or put into service AI systems in the EU, regardless of where those providers are established. The AI Act distinguishes between different types of rules to meet different types of risk levels, ranging from:

  - **Unacceptable risk AI** – Systems considered a threat to people will be banned outright. This will include systems that deploy subliminal manipulative techniques, exploit people's vulnerabilities or are used for social scoring (classifying people based on their social behaviour, socioeconomic status or personal characteristics).
  - **High risk AI** – These systems will be carefully regulated. Those that negatively affect safety and fundamental rights will have to be assessed before being placed on the market and throughout their life cycle.
  - **Low or minimal risk AI** – Systems that do not fit the "unacceptable" or "high" risk categories will have to comply with minimal transparency requirements (for example, informing users that they are interacting with an AI system).

The AI Liability Directive, meanwhile, will lay down "uniform requirements for certain aspects of noncontractual civil liability for damage caused with the involvement of AI systems". In certain circumstances, this will create a rebuttable presumption of causality, meaning that claimants seeking compensation will face a more reasonable burden of proof. National courts will also be empowered to order the disclosure of information on high-risk AI systems that are suspected of causing damage.

- Modernisation of the EU product liability regime with a new version of the Product Liability Directive (85/374/EEC) (PLD).

On 9 October 2023, a joint committee of the European Parliament agreed proposed amendments to the new PLD. The aims of the proposals include easing the burden of proof in complex cases, and ensuring there is always a business based in the EU that can be held liable for defective products brought into the EU from non-EU manufacturers. A new article would bring software into the scope of EU product liability laws (although software that is provided for free, or open-source, could be out of scope – under recital 13). As a wider range of economic operators could be defendants under this revised regime (including manufacturers of defective components, distributors, fulfilment service providers and online platforms), this may lead to an uptick in litigation as consumers make use of new powers of redress.

Developments in the UK

The UK government's Office for Artificial Intelligence issued its National AI Strategy guidance document in September 2021, highlighting the ambition to "remain an AI and science superpower fit for the next decade". The government's priorities for governing AI effectively were described as certainty for the UK AI ecosystem, improved public trust in AI, increased responsible innovation, and for the UK to maintain its position as a global leader in AI. It seems these priorities were not intended to be implemented legislation, with the National AI Strategy stating that there was "a big limitation in what can be covered in cross-cutting legislation on AI, and regardless of the overall regulatory approach, the detail will always need to be dealt with at the level of individual harms and use cases".

While the EU has set out various detailed legislative proposals, in March 2023, the UK government released a white paper outlining a proposed "pro-innovation approach" to regulating AI. No specific draft legislation for the regulation of AI was put forward. It is intended that, instead, existing regulators will be empowered to implement the following principles:

- Safety, security and robustness
- Appropriate transparency and explainability
- Fairness
- Accountability and governance
- Contestability and redress

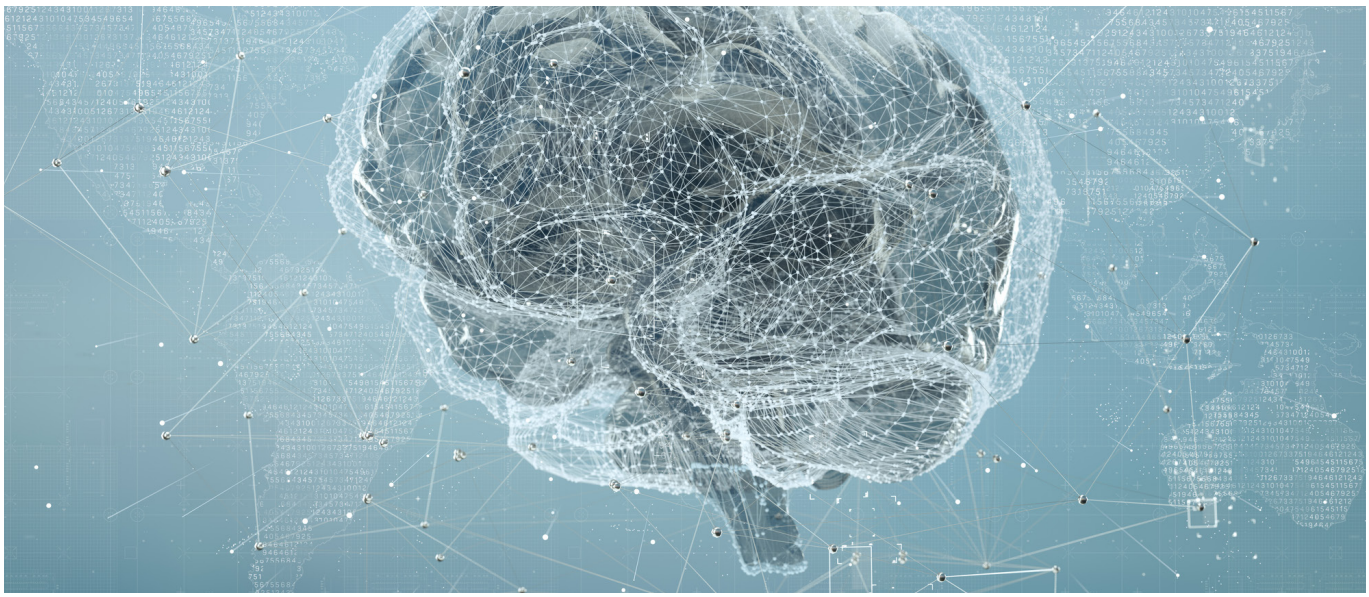
It is argued in the white paper that this approach will "[make] use of regulators' domain-specific expertise to tailor the implementation of the principles to the specific context in which AI is used." The UK government anticipates introducing a statutory duty on regulators to require them to have due regard to the principles, though there is no set timeframe for this.

In parallel though, the UK is also proposing to update its product safety regime and issued an OPSS consultation in August 2023, which specifically invites contributions from "small businesses in emerging sectors such as AI". However, the only specific question on AI in the consultation is one asking participants to provide examples of where the current product liability regime is "unclear because of technological developments (e.g. lack of clarity about who is responsible for safety of an AI/smart product or when software is updated)".

Publication of the replies to the consultation, and the government's response, are still outstanding, but the question suggests there may be AI-specific developments in updated UK product safety laws.

The government has already introduced broader legislation related to the security of connected devices. The Product Security and Telecommunications Infrastructure Act 2022 (PSTIA), relevant parts of which will come into effect on 29 April 2024, will require manufacturers of UK consumer connectable products to comply with minimum security requirements. These minimum security requirements are based on the UK's Code of Practice for Consumer IoT security and on advice from the UK's technical authority for cyber threats, the National Cyber Security Centre. A retailer will be a "distributor" under PSTIA and as such, we expect that they will have obligations to be "satisfied" that the conditions in the regulations are met, and not to supply products where they are aware that there is a compliance failure, but those sections of the PSTIA are not yet in force. However, there are sections in force that oblige the distributor to notify any known compliance failure to the authorities; and to take reasonable steps to remedy the failure, where they are aware or ought to be aware that the product is a "UK consumer connectable product".

In addition, in early November, Prime Minister Rishi Sunak launched the new AI Safety Institute, tasked with testing the safety of emerging types of AI. It will be interesting to monitor contributions from industry and governments, particularly on the points where interests diverge, and to see if the "non-legislative approach" envisaged in the white paper is still the preferred way forward, in light of the Bletchley Declaration.



Concluding Remarks

AI has existed for over 50 years, but it is the rate of recent progress and growing realisation of what it could deliver (and the risks of malfunction and general unpredictability) that has made its regulation a hot topic in 2023 and a debate that is almost certain to continue into 2024.

In the meantime, businesses should think about how they can manage risks of AI and legislation relating to AI in the context of their operation and products, and although this will largely depend on their own internal structures and processes, there are some key themes:

- **Assessing risks of products** – As with all products, risk assessments of AI or the use of AI with hardware/ other products, and how those assessments inform risk management models to ensure internal systems and supply chains deliver safe products to consumers, will be crucial.
- When thinking about the reasonable foreseeability of an AI product's use, developers should perhaps consider whether age-restrictions are appropriate. An unintended (but arguably foreseeable) consequence of some generative AI is the recent example in the US, where the photographs of around 30 underage high school students were manipulated, using AI, to generate pornographic images, perhaps a foreseeable misuse of the AI product, which potentially poses risk to the mental health of those targeted.
- **Incorporation of horizon scanning into risk management models** – Intelligence gathered from horizon scanning and other sources should be incorporated into risk management models, to ensure that its relevance for the development and use of AI in any particular business is properly assessed on an ongoing basis. Such horizon scanning might, for example, include monitoring reports of safety issues with similar competitor products that use AI or that originate from the same software developer, or new and emerging cybersecurity threats.
- **Awareness and ongoing monitoring of legislative changes** – Being aware of developing legislation relating to AI or relevant aspects of product safety in relevant markets, and how proposed new laws could impact a business, its products, its suppliers and/or customers, on an ongoing basis. Updates issued by trade associations, trade press and law firms could assist with such monitoring. This may also feed into the possibility of lobbying for regulatory alignment between different markets.
- **Compliance approaches** – If or when new legislation is introduced in one market but not in another, businesses may need to consider different approaches for managing the possibility of relevant products being noncompliant. For instance, the "highest" or "newest" standard could be applied on a global basis, or, alternatively, requirements could be managed separately for each market (although this would be more difficult for generative AI products or products that are available online, where it is more difficult to "restrict" a certain version of a product to a particular country).

Although some claim the fears around AI are being overplayed, even the more mundane uses of AI could have consumer safety implications, agreeing that a framework to protect consumer safety should perhaps be a priority for legislators, regulators and businesses alike. As it was put in the OPSS Report, "If an AI system works as intended, there is limited concern for its transparency. Challenges occur when something goes wrong."

One thing is for sure, AI looks set to transform the way we all do business, and consumer safety is a fundamental part of balancing those risks and benefits.

Contacts

Rob Elvin
T +44 161 830 5257
E rob.elvin@squirepb.com

Nicola Smith
T +44 121 222 3230
E nicola.smith@squirepb.com

Francesca Puttock
T +44 121 222 3215
E francesca.puttock@squirepb.com