Office for Product Safety & Standards

Update on OPSS Artificial Intelligence (AI) Research

Final Report

November 2024

This report was commissioned by the Office for Product Safety and Standards and prepared by the Centre for Strategy & Evaluation Services.

The views expressed in this report are those of the authors, not necessarily those of the Office for Product Safety and Standards (OPSS) or the Department for Business and Trade (DBT), nor do they necessarily reflect government policy.

Contents

Executive summary

The market for AI-driven consumer products continues to evolve, with increasingly complex AI applications being developed and deployed. These products can deliver significant benefits to consumers, such as enhanced safety and increased personalisation. However, there is also an emerging body of research highlighting the potential safety risks associated with the incorporation of AI into consumer products.

In this context, the Office for Product Safety and Standards (OPSS) commissioned the Centre for Strategy & Evaluation Services (CSES) to prepare this report, an update of the previous *Study on the Impact of Artificial Intelligence on Product Safety*, undertaken by CSES in 2021. In particular, the report explores: the key definitions of AI and new concepts; the market for AI consumer products; the product safety opportunities, benefits, challenges and risks; and regulatory and policy developments. It provides further insights on key issues and products through a number of case studies, as well as strategic considerations for OPSS.

There is no single **definition** of AI, with both variations in how the term is defined and also parallels between definitions. These variations can be largely attributed to the extensive number of applications and situations in which AI can be used, presenting a challenge in effectively defining AI in a general sense. However, authorities agree that AI systems display certain capabilities and characteristics, including the ability to generate outputs based on the inputs they receive, adapt their operations based on training data, and act and take decisions autonomously. The most important development since the previous study was published has been the widespread adoption and use of **frontier AI**, including large language models (LLMs), such as GPT-4. These models can produce content, including audio, code, images, text, simulations and videos. Further, there has been an increasing focus on identifying and tackling the risks and challenges associated with AI. For example, a number of states, including the UK, have established AI safety institutes.

The term AI continues to be conflated with other terms, in particular smart products. As such, it is challenging to determine the **exact scale and size of the market for AI consumer products**, since market data does not tend to distinguish between AI and non-AI consumer products. Market data usually refers to smart products, necessitating a closer examination of individual smart product categories to ascertain whether AI is integrated into certain consumer products. Nonetheless, the market for smart connected home devices, which **includes many AI-driven products**, remains strong, having grown by a third since 2017-2018. New AI-enabled products have emerged on the market, though many remain in their infancy. Smart wearables integrated with generative AI such as smart glasses, pins and monocles are coming to prominence, while developments in the field of robotics and AI offer increasingly improved functionalities personalised to consumers, assisting with chores and interacting with the user. The key adoption drivers of AI consumer products include **convenience, savings and personalisation** while the barriers remain **confidence in using the products, costs and privacy concerns**.

The **benefits** of AI consumer products include convenience, efficiency, enhanced personalisation and security. Predictive maintenance, a common feature of AI-enabled smart appliances, monitors their health and performance, ensuring timely repairs and component replacements. Further, consumer devices can contain security features, giving users control over their data and content, enhancing privacy. AI systems, due to their characteristics, have the potential to cause **material (physical) or immaterial (non-**

physical) harm. These could be, for example, an AI-driven robot malfunctioning, causing injury, or harm to privacy and reputation or psychological well-being. Tools are being developed to enable the reporting of incidents as awareness of the types of harms increases. However, as per the previous study, the research identified **limited evidence of concrete harms**. Many of the risks of harm remain theoretical in nature, and the potential harms remain greater than the actual harms.

Various **regulatory and policy developments** have taken place since the previous study, with different approaches taken as jurisdictions seek a fine balance between fostering innovation and ensuring safe, trustworthy and responsible AI. For example, **the UK, US, Singapore and Japan currently approach AI regulation in a non-statutory manner**, opting for guidelines and toolkits developed with industry. By comparison, the **EU, South Korea and China** have taken a hard law approach, introducing AI legislation. Some jurisdictions have indicated they will legislate the most powerful foundation models.

This report suggests that countries and international organisations should continue to **collaborate** at the bilateral and multilateral levels, **monitor** developments in AI and the application of regulatory and policy measures, and **engage** with various stakeholders, including consumers, industry, government agencies, academics and researchers, product safety practitioners and standards bodies. These actions can promote a shared understanding of AI, related harms and the views of different groups, as well as provide guidance on how to approach AI from a regulatory perspective.

1. Introduction

Study objectives and scope

The overarching aim of this report is to **provide OPSS with an updated landscape of AI relevant to OPSS remit/areas of responsibility in product safety**, building on the previous scoping study undertaken by CSES in 2021, *Study on the Impact of Artificial Intelligence on Product Safety* (OPSS, 2021a). This report should be considered an addition to the aforementioned study. For a comprehensive understanding, the relevant sections of the study should be viewed but a brief summary of the previous findings is presented in the box at the beginning of each section of this report. The report aims to achieve the following three specific objectives:

- **Objective 1:** Provide an update on current and future applications of AI in consumer products (exploring benefits and harms (physical and non-physical) that it will bring to the consumer), how this will impact consumer safety and how AI may be used in product design / maintenance / updating.
- **Objective 2:** Based on the updated landscape, understand the current risks and hazards for a new generation of products incorporating AI within the current regulatory frameworks (for the defined scope of products).
- **Objective 3:** Inform what regulators should consider and actions required to respond to these new challenges to ensure consumers are kept safe whilst not stifling innovation, in line with the principles-based approach set out by the Department for Science, Innovation & Technology (DSIT) in its white paper *A pro-innovation approach to AI regulation* (DSIT, 2023). These principles are: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.

Considering the report **scope**, all manufactured consumer products subject to the General Product Safety Regulations (GPSR) 2005 and other relevant legislation for specific goods are covered (e.g. Electrical Equipment (Safety) Regulations 2016, Electromagnetic Compatibility Regulations 2016, Radio Equipment Regulations 2017 and Toys (Safety) Regulations 2011). The scope does not include vehicles, medicines and food products, in line with OPSS' remit, and does not cover the use of AI by regulators, or its use in construction products.

The key **outcome** of the report is to provide OPSS with an (updated) understanding of product safety issues related to the current and future incorporation of AI in consumer products, as well as conclusions and suggestions on possible regulatory next steps. This report is based on desk research only. As such, engagement with stakeholders interested in AI and consumer product safety could provide greater insight than desk research alone, in what is a rapidly evolving area. The research was conducted between May and September 2024.

2. Understanding Artificial Intelligence

This section examines the key terminology related to the integration of AI in consumer products. It provides definitions of AI and machine learning, before outlining newer terminology that has developed in recent years. The second sub-section provides an overview of recently published definitions by institutional actors in the UK, such as DSIT and the Home Office, as well as the European Commission, the National Artificial Intelligence Initiative (USA) and the OECD. A summary of the findings from the 2021 study has been provided in the box below (OPSS, 2021a).

According to the Government Digital Service (GDS) and the Office for Artificial Intelligence, **AI can be defined as "the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence.** AI is constantly evolving, but generally it: involves machines using statistics to find patterns in large amounts of data; and is the ability to perform repetitive tasks with data without the need for constant human guidance" (GDS and Office for Artificial Intelligence, 2020). Tasks that AI systems can perform can be specific, also called 'weak' or 'narrow' AI (e.g. optimising electricity usage on a smart grid), or 'general' (e.g. an advanced chatbot).

AI processes vast amounts of data, that might originate from various sources, such as images, video, sound or text, through algorithms that draw conclusions, adjust parameters and produce outputs.

Examples of the uses of AI in consumer products include:

- Facial recognition as a security feature on devices, such as mobile phones.
- Smart speakers, which use speech recognition to ascertain requests by digitising vocal sounds into a machine-readable format and analysing the words to determine what a consumer requires.
- Generative text processing or image creation using human prompts.

Machine learning (ML) is a subfield of AI that gives computers the ability to learn "without being explicitly programmed" (Samuel, 1959). Some examples of applied ML include the classification of images into different categories, natural language processing (NLP), and healthcare diagnosis. The 2021 study presents a detailed explanation of the ML design and development process.

Terminology: explaining artificial intelligence and new concepts

The purpose of this section is to introduce terminology and practices associated with AI and ML that have been developed in the years since 2021. Practices have evolved and it is therefore important to consider new technologies in the field of AI to understand the risks associated with them when they are integrated into consumer products.

The most important advancement in this time period has been the widespread adoption and use of **frontier AI** (DSIT, 2023b). This term describes AI models that have been trained on broad data sets and fine-tuned for specific tasks. Some of them are large language models (LLMs), trained on large amounts of text to imitate human language. Examples of widely used products include GPT-4 and DALL-E. Often embedded within chatbots, such as ChatGPT, these models can be used to generate text, images and videos in response to prompts, thereby creating a conversation with the user. Key potential uses of this technology include:

- **Content creation and writing**: Assisting writers in brainstorming new ideas, generating creative writing. Journalists may also use them to generate articles and news pieces (Brown, T. B. et al., 2020). Students can also use the tools in the same way, or to correct errors in texts they have already written. Language learners may also use generative writing tools to sharpen their language skills and learn commonly used phrases.
- **Design and art**: Generative image software can create images, video and music based on text prompts. This is the case for DALL-E. It can be useful for graphic designers and artists (Orksanen, A. et al., 2023), or user interface/user experience (UI/UX) designers, who can use these tools as a basis for further creation.
- **Customer support and chatbots**: Companies can use foundation model-based chatbots to answer questions and queries on their products or services (Argyle, L. P. et al., 2023).
- **Healthcare and medicine**: Models can assist in medical documentation, research, and patient communication (Wang, J. et al., 2022).
- **Programming and code generation**: Programmers can use tools such as GPT-4 to help write code, explain programming concepts and debug issues, which can save time (OpenAI, 2021).

The advancements in frontier AI models reinforce the challenges of defining and classifying AI systems highlighted in the 2021 OPSS study, which found that different AI systems display different levels of the core AI characteristics – classified in that study as autonomy, data needs, opacity and mutability.

In this context, efforts have been ongoing to classify from a technical perspective the different levels of capabilities provided by AI systems. For instance, the below table illustrates a matrix approach to classifying systems on a path to artificial general intelligence (AGI) based on their performance and generality of capabilities (Morris et al., 2024). While the assignment of examples to categories is approximate, as there is no standardised benchmark, this categorisation illustrates the following:

- **Narrow AI** – applications, including consumer product examples, span all levels of performance.
- **General AI** – applications are still limited to Level 1 in terms of performance.

Table 1: Example matrix classification of progress towards artificial general intelligence

Performance (rows) x Generality (columns)	Narrow	General
Level 0: No AI	**Narrow Non-AI**	**General non-AI**
Level 1: Emerging (equal to or somewhat better than an unskilled human)	**Emerging Narrow AI** *GOFAI (Boden, 2014); simple rule-based* *systems, e.g., SHRDLU (Winograd, 1971).*	**Emerging AGI** *ChatGPT (OpenAI, 2023), Bard (Anil et al., 2023), Llama 2 (Touvron et al., 2023), Gemini (Pichai & Hassabis, 2023).*

Performance (rows) x Generality (columns)	Narrow	General
Level 2: Competent (at least 50th percentile of skilled adults)	**Competent Narrow AI** *Smart Speakers, such as Siri (Apple), Alexa (Amazon), or Google Assistant (Google).*	**Competent AGI** *Not yet achieved*
Level 3: Expert (at least 90th percentile of skilled adults)	**Expert Narrow AI** *Generative image models such as Imagen (Saharia et al., 2022) or Dall-E 2 (Ramesh et al., 2022).*	**Expert AGI** *Not yet achieved*
Level 4: Virtuoso (at least 99th percentile of skilled adults)	**Virtuoso Narrow AI** *Deep Blue (Campbell et al., 2002), AlphaGo (Silver et al., 2016).*	**Virtuoso AGI** *Not yet achieved*
Level 5: Superhuman (outperforms 100% of humans)	**Superhuman Narrow AI** *AlphaFold (Jumper et al., 2021), StockFish (Stockfish, 2023).*	**Artificial Superintelligence (ASI)** *Not yet achieved*

Source: Adapted by the authors from Morris et al., 2024.

Additional practices, techniques and concepts that have emerged as important in the field of AI/ML since 2021. Focused on explaining, as well as tackling, the risks and challenges associated with AI/ML, these include:

- **AI safety**. An interdisciplinary field defined by the UK Government as “the understanding, prevention, and mitigation of harms from AI. These harms could be deliberate or accidental; caused to individuals, groups, organisations, nations or globally; and of many types, including but not limited to physical, psychological, social, or economic harms” (DSIT, 2024).
- **Neuro-symbolic AI**. This term describes applications that seek to combine the efficiency of neural networks with the “rules, logic and reasoning” (Belle, no date) of ‘symbolic’ AI to improve interpretability and problem-solving.
- **Prompt engineering** is the process of designing prompts to efficiently utilise LLMs like GPT-4 (OpenAI, no date). This phrase has been a talking point for several years now, especially in terms of changes in the way people work and study, given the use of AI tools will be an important skill in the coming years.
- **Federated learning** refers to methods that train AI models across multiple devices while keeping data localised, thereby enhancing privacy (Banabilah, S. et al., 2022).
- **Explainable AI** (XAI) concerns techniques and methods aimed at making AI decisions understandable to humans (Ali, S. et al., 2023).
- **Alignment** refers to the extent to which an AI’s goals align with its creators’ goals (Gent, E., 2023).

- **Hallucination** describes the tendency of AI chatbots to confidently present false information (MIT Management, no date).

Key definitions published since 2021

New definitions have also been put forward in recent years by institutions, in the UK, as well as by the EU and other international organisations. This subsection presents an overview of these definitions.

In the UK, the **Department for Science, Innovation and Technology (DSIT)** has particular responsibilities for AI-related topics. In March 2023, it published an *Artificial Intelligence Sector Study* (DSIT, 2023a), which delved deeper into the AI industrial sector, and re-explained the definition of AI initially described in the 'National AI Strategy' (DSIT, 2021). In essence, AI is described as the "fastest growing deep technology in the world, with huge potential to rewrite the rules of entire industries, drive substantial economic growth and transform all areas of life" (DSIT, 2021).

While recognising the challenges, limitations and questionable value of trying to tightly define AI, DSIT's pro-innovation approach to regulating AI defines AI as "a general-purpose technology like electricity, the internet and the combustion engine" (DSIT, 2023). It points to the core characteristics of AI as the 'adaptivity' and 'autonomy' of the technology – i.e. that AI technology can operate based on instructions that have been learnt rather than programmed, and that can be autonomously applied within dynamic and fast-moving environments.

Moreover, DSIT provided a more detailed explanation of its definition of AI in its policy paper *AI regulation: a pro-innovation approach* (DSIT, 2023). Recognising that "there is no general definition of AI that enjoys widespread consensus", DSIT reinforced the UK Government's focus on the following two characteristics:

- **Adaptivity**, stating that AI systems are 'trained' and operate by inferring patterns and connections in data that are often not easily discernible to humans. This may allow them to develop the ability to perform new forms of inference not directly envisioned by their human programmers. Accordingly, this characteristic can make it difficult to explain the intent or logic of a system's outcomes.
- **Autonomy**, stating that some AI systems can make decisions without the express intent or ongoing control of a human. This characteristic can make it difficult to assign responsibility for outcomes.

Other similar yet slightly different visions of AI are used throughout Government. For example, the **Home Office** has put forward the following aspects: AI means the simulation of human intelligence by machines (including computer systems), which have the ability to perform tasks that demonstrate learning, decision-making, problem solving and other tasks which previously required human intelligence. It includes 'machine learning', 'deep learning' and 'large language models'. Defining AI in this context aims to help stakeholders understand how the technology could be used in harmful ways (Home Office, 2023). Examples include the generation of synthetic child abuse material, actors committing fraud and generating deepfake revenge pornography, among other threats.

Expanding the scope to other international institutional actors, in April 2021, the **European Commission** proposed the first EU legal framework to regulate AI. Following this draft, the European Parliament adopted the 'AI Act' in March 2024 (EU, 2024). The understanding of AI included in this Act is clearly defined in Article 3 of the legislation:

*'AI system' means a machine-based system that is designed to operate with varying levels of **autonomy** and that may exhibit **adaptiveness** after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments* (EU, 2024)

This is further supplemented by the text of Recital 12, which states that: "the definition should be based on **key characteristics of AI systems** that distinguish it from simpler traditional software systems or programming approaches", further noting that "a key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing, enables learning, reasoning or modelling".

In this regard, the UK and EU definitions cover similar ground in their references to the **autonomy** and **adaptiveness** of AI systems, as well as the importance of their capability to produce outputs based on **inferences**.

The **United States**, through its National Artificial Intelligence Research Resource (NAIRR) Task Force, published the following definition in January 2023: "the term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human based inputs to:

- Perceive real and virtual environments.
- Abstract such perceptions into models through analysis in an automated manner.
- Use model inference to formulate options for information or action." (NAIRR Task Force, 2023)

Finally, the **OECD** has determined that the following definition was the most relevant for the context in which it operates:

"*An AI system is a machine-based system that, explicit or implicit objectives, **infers**, from the input it receives, how to generate outputs such as, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of **autonomy** and **adaptiveness** after deployment*" (OECD, 2023).

This definition (and its update) comes from the fact that the organisation has ruled with consensus and has therefore used the knowledge of many experts and country representatives to arrive at this definition. In line with the UK and EU definitions, the OECD highlights the importance of the levels of autonomy and adaptiveness present in AI systems, as well as their ability to infer in the generation of outputs.

The broad range of definitions is a marker of the importance of different parameters in each case's objectives. In reality, this technology forms the basis for a large number of build and use cases, which makes it difficult to define effectively in a general sense. All in all, the goals of the different government bodies and institutions are to characterise the systems while allowing for future innovation and developments in this sector. This explanation applies especially to consumer products with embedded AI.

As stated by DSIT, no general definition of AI enjoys widespread consensus, largely due to the extensive number of applications and situations in which AI can be used. However, significant work has been done since 2021 to further explain AI in specific contexts. This is particularly true in the area of policy and legislation, where the UK government, as well as the EU, the OECD and others have outlined their understanding of AI and its regulatory implications.

It is also true in a technical sense, where the advancements in ‘frontier AI’ models, including LLMs, are a key development, and focus is being placed on the classification of progress towards advanced artificial general intelligence.

In defining AI, these authorities generally highlight similar capabilities and characteristics. These include the ability of AI systems to: (i) infer how to generate outputs based on the inputs they receive; (ii) adapt their operations based on ‘training’ such that the outputs and outcomes are not easily interpreted and/or not directly envisioned by humans; and (iii) act and take decisions autonomously. To add further complexity, individual AI systems can exhibit each of these three characteristics at different levels.

While consideration of the specific situation of AI in consumer products continues to receive limited attention, it can be concluded that these developments largely reflect the core findings of the 2021 OPSS study. Specifically, the findings on the key characteristics of AI that are most relevant with regard to the risks of integrating AI systems into consumer products. The only amendment relates to the consideration of the opacity of AI systems not as a core characteristic of these systems, but as a result of the adaptivity of AI systems – i.e. their ability to generate outputs and outcomes that are not easily interpreted or explainable by humans.

3. Market for AI consumer products

This section provides an update on the market for AI consumer products. It considers AI consumer products already on the market, as well as those that could emerge over the next 10 years. In particular, it examines: (i) the types of AI applications in use; (ii) the scale of use of AI across consumer product groups; and (iii) the future development of the market. A summary of the findings from the 2021 study has been provided below.

The 2021 study found that the **market for AI consumer products was characterised by continuous growth, but faced a challenge in assessing the true scale and dynamics of the market**. AI, often used as a buzzword in product marketing, is commonly conflated with related terms such as 'smart' products, 'connected' products and consumer Internet of Things (IoT) products. The data did not specifically provide information on the scale of AI consumer products as a cohesive market; however, data on the market for and usage of AI products in some categories was identified. Barriers to the adoption of these products included costs, privacy and awareness, though overall the use of AI consumer products was found to be increasing.

The market for AI consumer products continues to grow both in the UK and globally, as AI technologies evolve and more sophisticated products are placed on the market. However, the term AI continues to be conflated with other terms, most notably smart products. This section considers the market for AI consumer products specifically, providing examples of products, the types of AI used and their capabilities. For a comprehensive analysis of both AI and non-AI consumer products (both categorised as smart products), please refer to Annex 2. The evolving market for AI-driven consumer products is increasingly mirrored in the different types of AI applications, and increasing capabilities, being developed and deployed. AI consumer products range from those using quite simple algorithms to more complex models. Developments in the field of AI are reflected in the **increasingly complex applications used by AI consumer products** on the market. These developments are intended to improve the effectiveness and efficiency of AI consumer products, increasing their convenience for consumers.

Smart speaker ownership has increased significantly in recent years. Smart speakers, with their natural language processing (NLP) abilities, use speech recognition to understand and respond to user requests, allowing for clear conversations with users. The algorithms utilised by smart speakers, embedded in the cloud, constantly learn from voices, commands and conversations. Traditional tasks undertaken by smart speakers include turning on lights, playing music, searching for information on the Internet and making phone calls.

As illustrated in section 2, a major development since the previous study has been **the emergence and increasing prominence of generative AI models**, particularly since the release of ChatGPT in November 2022 and subsequent and constant iterative technological advancements. Generative AI models can produce content, including audio, code, images, text, simulations and videos. Research has suggested that generative AI applications could add up to USD 4.4 trillion (GBP 3.5 trillion) annually to the global economy (McKinsey & Company, 2024).

The incorporation of generative AI algorithms is now **transforming the smart speaker segment**. Last year, it was announced that the major voice assistant Alexa would be powered by a new LLM to improve its capabilities, understand and interpret conversational phrases more effectively and respond appropriately, carrying out various requests from one command (Tuohy, 2024). Recognising the value of voice communication, the new LLM is specific to voice interactions, improving a number of capabilities (Newman, 2023).

The upgraded voice assistant has improved conversation, including the ability to understand non-verbal cues and reduced latency, enhancing conversation flow without pauses. Another improvement is the ability to build complex tasks in one statement without the need to turn several devices on and off individually. Additionally, the voice assistant has become more personalised, remembering context and allowing for fluid conversation. For instance, a user can ask a question about a restaurant and carry on the conversation to obtain directions and opening times. The new LLM intends to give the voice assistant more of a personality as well, such as offering opinions (Newman, 2023).

With the implementation of the new LLM and the emergence of generative AI in this upgraded voice assistant, it will be interesting to understand how the developments will change the way users interact with it in the long term (Newman, 2023). It has even been suggested that, with voice assistants being able to better utilise collected data, they will understand a user's routine and act accordingly, such as making coffee or watering the lawn. The assistant could even function without voice command, becoming an autonomous assistant that understands the needs of a user. In this context, **generative AI promises to offer enhanced capabilities in voice assistants** and, with further investment and innovation, users can expect broader capabilities (insideBIGDATA, 2023).

Smart domestic appliances such as refrigerators and ovens are also embracing the power of generative AI to improve product features and enhance consumer experience (Marr, 2024). GE Appliances, for example, has developed an app leveraging LLMs to analyse ingredients a user has in their refrigerator to create recipes, simplifying cooking, saving money and reducing food waste. Another manufacturer, Samsung, is planning to incorporate generative AI into smart refrigerators and ovens, for example to recognise what is being cooked, enabling the appliance to understand consumer needs and respond accordingly (Samsung, 2024). While it is presently unclear how the features driven by generative AI will function, potential ideas include smart ovens providing notifications to improve cooking conditions and parameters, or fridges delivering recipes from ingredients that need to be used. The incorporation of generative AI into these products is a relatively new phenomenon (Marr, 2024).

Another firm, Miele, is deploying cameras in large ovens to take pictures, before using generative AI to interpret them and suggest the cooking mode. AI is also being used for appliance diagnostics to assist customers when there are malfunctions, such as a smart washing machine creating too much foam. In this case, the AI system would suggest the correct amount of detergent for the load amount. **Maintenance is a feature of AI-driven domestic appliances**, which can predict issues in advance of them occurring. As such, generative AI can order replacements, schedule technician appointments or even provide troubleshooting guides, specific to the model and its conditions (Marr, 2024).

In 2023, 8% of consumers claimed to own a smart washing machine (increasing from 1% in 2017), while smart refrigerator ownership stood at 4%. Ownership of smart kettles/smart coffee makers was 6% and smart oven/hob ownership was 4% (techUK, 2023). As such, **ownership levels remain very low** and should be taken into account when considering the potential impact of risks associated with AI-driven domestic appliances, as more conventional, non-smart domestic appliances continue to dominate the market.

New developments have also taken place in the smart wearables category, with AI-powered sunglasses, pins and monocles coming to prominence. Ray-Ban Meta's smart glasses can take videos and photos and, using generative AI that can process information across image and text in the cloud, analyse them and respond accordingly, for example to identify and describe an object (Ghaffary, 2024). The user can also ask the sunglasses for English translations of foreign signs, or ask for a caption to accompany images, with the list of functionalities set to grow over time. At present, the sunglasses are only available in the US and Canada (Meta, 2024a). However, it has been suggested that prolonged use of smart glasses may cause eye strain and discomfort because of the short distance between the screens and eyes. Blue light from the glasses can disrupt sleep, leading to insomnia and other sleep-related issues. Additionally, distractions caused by glasses could lead to accidents, since glasses can reduce situational awareness (Baba, 2023).

Humane AI's pin, which uses the LLM GPT-4, can translate, read messages and ask questions about objects, providing personalised responses. For example, if the user has a food allergy, they can pick up a food item, tap the pin and ask if they should purchase the item. The pin then responds according to whether it was able to determine if the food item contains an allergen. Although the pin does not have a screen, it can produce a display through projecting light onto the user's hand. Orders began shipping early in 2024 (Dotson, 2024). AI-driven monocles, which fit onto the user's glasses, offer similar features, such as translations and answers to simple questions. Written responses are provided on an embedded AR screen (Jewiss, 2023). However, the pin has received negative reviews, with consumers commenting on its functions, criticising its battery life and questioning its overall utility, particularly with regard to it replacing the smartphone. It has been suggested that, while the pin and similar devices offer some insight into what AI could bring in future, they have not yet delivered (Kleinman, 2024).

While these **inventions are attempting to challenge the smartphone**, it is unlikely that smartphones will disappear. Smartphone manufacturers are constantly modifying their products with more AI features, and even more explicit AI branding, and there is a question as to whether there is a need for these new products or whether their functionalities can simply be built into smartphones (Ghaffary, 2024).

Robotics is another field which is increasingly utilising AI to improve functionalities personalised to the user, such as in entertainment, healthcare, transport and domestic chores. Examples of developments in the field include:

- Jizai Arms has developed robotic limbs, consisting of six arms, that can be controlled by the user to perform an array of tasks, ranging from use in a warehouse to a surgery room to a consumer environment. In fact, the robotic arms could have the most impact for those with disabilities. Acting as a replacement for those with missing limbs, they would allow the user to carry out tasks that would otherwise be too difficult (Papadopoulos, 2023).
- Google DeepMind has developed a self-improving AI agent for robotics that can undertake various tasks and self-generate new training data to improve. Based on their multimodal model, which processes languages, images and actions, and combined with a large training dataset of various robotic arms carrying out hundreds of tasks, it is set to accelerate robotics research, reducing the need for human-supervised training towards creating a general-purpose robot (Google DeepMind, 2023).

- In recent years, Boston Dynamics has partnered with Meta to advance the robotics field. The robots are trained with simulation data with the aim of following generalised instructions, solving problems by themselves, and navigating the physical world autonomously, retrieving physical objects. However, given the limited data available to physical robots compared to AI chat bots, for example, it will likely still be some time before generalised robots are commonplace in the real world (Boston Dynamics, n.d.).
- LG has developed an AI-driven robot to help with daily chores that possesses autonomous mobility, advanced communication and engaging functions. With NLP ability, the robot recognises users, can understand and express emotions, and interact verbally, enabled by built-in sensors, a camera and a speaker. For example, it can greet a user, detects their emotions and select music or other content to suit their mood. The robot also operates as a smart hub, enabling the user to connect with and control other IoT devices (Sood, 2023).

While the market for AI-driven robotic devices is growing in terms of applications and number, it has been suggested that consumers will experience the benefits of domestic robots by 2030 (Gupta, 2024). Indeed, experts from the UK and Japan have suggested that 39% of time currently spent on domestic chores could be automated within the next decade (PLOS, 2023). **Many of these products are still in their infancy** but, as with the wider market for AI consumer products, it will be interesting to see how their growth develops in the coming years, as well as the impact on consumers. Indeed, while key adoption drivers include convenience, savings, personalisation, compatibility with other devices, as well as confidence in using the products, product costs and privacy concerns remain barriers to adoption (techUK, 2023).

Over the next 5-10 years, these products are likely to emerge on the market. Applications of AI in consumer products are becoming increasingly complex, particularly with advancements in generative AI. Generative AI, perhaps the biggest development since the previous study with its ability to produce content, is transforming AI consumer products. While it is not possible to determine the exact AI consumer products and functionalities that will be available in future, it has been suggested that smartphones could become primarily AI assistants, helping individuals with organising their lives and accessing data as and when needed, beyond the capabilities of current handsets. By 2035, domestic robots could be commonplace. In particular, personal robots could be used regularly by the elderly, infirm or those with disabilities, while they could also be used for daily chores or providing security (Marr, 2024a). AI is more prevalent in consumer products now compared to 2021, primarily because new products have emerged, such as smart glasses, as well as the increasing use of generative AI. However, the exact scale of the market should not be overestimated given estimated low ownership levels.

4. AI consumer products: product safety opportunities and risks

This section assesses the product safety opportunities, as well as the risks and challenges arising from the incorporation of AI systems into consumer products. Considering the risks in particular, it aims to demonstrate what the risks are, the potential scale of the risks, and the likelihood and severity of the risks and any resulting harms, including the extent to which they have been observed in practice or are theoretical in nature. A summary of the findings from the 2021 study has been provided below.

The incorporation of AI systems into manufactured consumer products brings opportunities, as well as challenges and risks.

Specific to product safety, the **direct opportunities** include: more efficient and effective products; and predictive maintenance capabilities, which can improve product safety, and reduce maintenance costs and product downtime. **Indirect opportunities** include: improved data collection and analysis to improve product quality; improved cyber security protection; AI powered product design; and more personalised products.

Considering the **challenges, risks and resulting harms**, the report found that core characteristics of AI as a technology (including mutability, opacity, data needs, and autonomy) can lead to errors in AI systems that have the potential to cause harm. These challenges can be categorised into themes, including robustness and predictability, transparency and explainability, security and resilience, fairness and discrimination, and privacy and data protection. Potential harms, resulting from these challenges, can also be categorised, broadly as material or immaterial in nature. Material harms are more likely to occur as a result of challenges in the first three themes (robustness and predictability, transparency and explainability, security and resilience). These could include, for example, an AI-driven robot malfunctioning due to automated decisions causing physical injury, or cyber security vulnerabilities leading to threats to physical safety.

To date, many of the risks are theoretical in nature and evidence of real examples of harms caused by AI consumer products is lacking. The limited evidence is likely due to the lack of maturity of consumer products incorporating AI, the consideration of safety impacts by manufacturers and developers, and the difficulty understanding the role and impact of AI systems when incidents occur.

Opportunities and benefits

The principal value of AI systems remains their **ability to display human-like capabilities**, such as reasoning, learning, planning and creativity, and make predictions and decisions, carrying out tasks normally performed by humans. Processing vast amounts of data, AI can achieve positive product safety impacts throughout the value chain, leading to enhanced safety for consumers. AI-driven improvements in the manufacturing processes, as well as the use of AI in consumer products, identifying unsafe product usage or optimising product performance, can improve product safety, raising consumer trust levels.

AI-powered smart and connected products can offer consumers improved convenience, efficiency and security, **leading to a number of direct benefits**. AI can offer highly personalised user experiences, understanding user needs and adjusting settings accordingly by analysing data on habits, preferences and usage patterns. For example, smart speakers can identify individuals and provide personalised information, as well as taking actions like adjusting the temperature or a playlist based on preferences. Another benefit of AI technology is its ability to analyse energy consumption and optimise usage, reducing energy waste and costs. AI can facilitate improved energy management by controlling heating, cooling and appliance usage based on data and user preferences. Headphones incorporating AI allow users to select which background noises to block out and concentrate on one specific voice, improving hearing health and enjoyment (Sparkes, 2024). Smartwatches with AI analyse and monitor users' health, while allowing them to schedule events, access the news and play music, among other tasks (Medical Device Network, 2023).

Predictive maintenance is another key advantage of integrating AI. With the ability to monitor the health and performance of consumer devices in real-time, this AI functionality is one of the more commonly deployed features, enabling the efficient and effective use of AI-enabled consumer products. Predictive maintenance allows organisations to forecast the performance status of equipment to ensure its repair can be scheduled in a timely manner. By establishing when an intervention is needed, predictive maintenance can play a key role in preventing accidents from occurring due to product malfunctions or failures. Using the example of the smart washing machine, predictive maintenance can facilitate the ordering of replacements and scheduling of technician appointments. Through analysing sensor data and device diagnostics, algorithms recognise patterns that suggest imminent malfunctions and alert users or service technicians. It can also provide guidance specific to the model.

AI-powered systems can also improve home security, using facial recognition technology and anomaly detection to identify and flag the identification of objects to the owner. Another benefit of the use of AI in consumer products is its ability to collect data and analyse user interactions, enabling developers to review and improve their products. With key insights into consumer behaviours and preferences, companies can adapt their products to suit the needs of their customers (Kvartalnyi, 2024). For example, AI can learn and adapt to user routines, enabling enhanced energy management, reducing waste and lowering costs while maintaining comfort. Similarly, AI consumer products can learn from user habits and automate routine tasks, such as turning off lights when not required or operating a coffee maker when the user wakes up (Mazur, 2024).

Considering the security and safety features of AI consumer products more closely, there are different ways in which **AI can heighten consumer protection and enhance user experience**. The use of predictive maintenance in smart washing machines has been mentioned already, and can ensure their effective and efficient functioning through continuous monitoring. Smart glasses can enhance road safety through driver assistance and alerts. Using sensors and algorithms, the glasses can detect potential hazards such as pedestrians, cyclists, or other vehicles. Providing timely alerts, the driver can react quickly and avoid accidents. In addition, the glasses can monitor driver fatigue levels and notify the driver, but there remain challenges. Distraction has been cited as one, with the risk that drivers become over reliant on the information provided by the glasses (or respond to inaccurate information provided by the AI). Another challenge posed by the glasses is widespread adoption by the general public, who may be sceptical in using them.

However, with technology continuously evolving, smart glasses have the potential to improve road safety and overall driving experience (Sanghi Transport Company, 2023).

Smart glasses also offer the user **control over their data and content**, with settings facilitating how the user manages their information and the content shared with others. They also offer an auto-lock contacts feature, allowing voice command to unlock contacts through a paired device, thus providing an added layer of security. The user can choose whether to store voice recordings or delete voice interactions. While these features have been designed to ensure a more secure experience, with better safety and privacy settings to enhance consumer use (Meta, 2024), the long-standing challenge of complex privacy controls may limit such benefits (e.g. Keith, M. J. et al., 2014).

Similarly, **smart speakers offer features that aim to mitigate data privacy risks**. For instance, an individual can simply mute the microphone when not using the device, and delete recorded interactions. Additionally, smart speakers allow the user to control whether the device sends information to the manufacturer to help improve product performance. These functions can be considered important, particularly with research having found that smart speakers often record by mistake, or that manufacturers have allowed employees or contractors to listen to recordings for the purpose of improving speech recognition (St. John, 2022). Other actions that can be taken to improve privacy and security include deactivating personalised features to hinder access to data by others, or enabling two-factor authentication (2FA) (Kaspersky Lab, no date).

AI consumer products are incorporated with a number of features to improve user convenience, satisfaction and security. While the benefits and opportunities of AI consumer products are evident, there are a range of challenges and harms that could result from their use.

Challenges and risks

The previous study considered **key characteristics** of AI that have the potential to cause challenges, which could result in consumer harm. These characteristics were:

- mutability (which can be considered analogous to the concept of adaptiveness highlighted in the definitions of key regulators outlined in section 2);
- opacity;
- data needs; and
- autonomy.

The study found that these characteristics could lead to certain **challenges**, which were categorised according to different themes, including:

- robustness and predictability;
- transparency and explainability;
- security and resilience;
- fairness and discrimination; and
- privacy and data protection.

These challenges, in turn, have the potential to cause **material (physical) or immaterial (non-physical) harms**.

The harms presented in the previous study remain, whether theoretical or otherwise in nature. Examples include an AI-driven robot malfunctioning and causing physical injury, or harms to one’s privacy and reputation or psychological well-being. However, as the intention of this report is to provide an update of the research, it does not restate the previous study's findings. Instead, it focuses on new challenges and risks that have emerged in the intervening years.

Further research conducted since 2021 has sought to provide a more comprehensive understanding of AI harms and the types of harm. The OECD (2024) recently published a report that aims to present a categorisation of the types of AI harm without being too prescriptive. It distinguishes between an '**AI incident**', an event where an AI system results in actual harm, and an '**AI hazard**', an event where an AI system is potentially harmful.

More specifically, "an AI incident is an event, circumstance or series of events where the development, use or malfunction of one or more AI systems directly or indirectly leads to any of the following harms:

1. injury or harm to the health of a person or groups of people;
2. disruption of the management and operation of critical infrastructure;
3. violations of human rights or a breach of obligations under the applicable law intended to protect fundamental, labour and intellectual property rights;
4. harm to property, communities or the environment." (OECD, 2024)

An AI hazard is defined as an event that "could plausibly lead to an AI incident", with the same types of harm listed. Psychological harms and harms to mental health are included under health in the first point, while reputational harm to individuals and other intangible harms such as hate speech, misinformation and disinformation are included under the third point in relation to fundamental rights. While potential harm is often defined as the risk or likelihood that harm or damage will occur, actual harm is a risk that materialised into harm, generally focusing on physical injury or damage to health, property or the environment. The term actual harm is often associated with incident. However, the report clearly states that the definitions "aim to foster international interoperability while providing flexibility for jurisdictions to determine the scope of AI incidents and hazards they wish to address" (OECD, 2024). Moreover, the OECD's categorisation is broader than the use of AI in consumer products.

The **types of harm** are listed, where an AI incident can result in the following:

- **Physical harm**: This can be categorised by type or severity of the injury.
- **Environmental harm**: This can be categorised by type of environmental damage (e.g. soil contamination, air pollution, or water pollution).
- **Economic or financial harm, including harm to property**: This can be categorised on the basis of scale of financial loss or damage.
- **Reputational harm**: Individuals can be impacted by reputational harm. An organisation's reputation or public trust in that organisation can also be harmed.
- **Harm to public interest**: This includes harms to critical infrastructure and functions (e.g. political system and the rule of law). Harms to the social fabric of communities are also included.
- **Harm to human rights and to fundamental rights**: This includes harms to privacy rights, for example.
- **Psychological harm**: Psychological harm and harm to mental health are being increasingly included in standards and product safety legislation. Psychological harm is more difficult to assess and quantify than physical harm.

In the context of AI consumer products, **some of these harms are more relevant than others**, whether theoretical in nature or actual occurrences. According to the typology above, defects in the functioning of household devices and appliances are more likely to result in physical and psychological harms than environmental harm, while harms to the public interest are more likely to occur due to malfunctioning large-scale AI systems. However, outlining the different types of harms can facilitate a more comprehensive understanding of the harms that could occur, their likelihood, and their scale as a result of the use of AI in consumer products.

It should be pointed out that the OECD's report aims to support a common AI incident reporting framework and the AI Incidents Monitor (AIM), which seeks to capture real-life examples of different types of AI harm (OECD, 2024a). As such, **the approach to reporting has not yet been fully developed**, which perhaps reflects not only the relatively new nature of AI-related harms, but also ongoing discussions around how they can be mitigated and the relative scale of the harms.

AIM tracks AI incidents and hazards reported in reputable media sources, and classifies them according to a range of variables, such as type of harm, severity, country, and industry. Usefully, the latter variable includes 'consumer products' as a category. Although the events reported are only likely to reflect a subset of incidents and hazards globally, AIM can be considered **a helpful starting point for providing the evidence base** to support the reporting framework and policy discussions. At present, the tool does not facilitate open submissions, court judgments and supervisory body decisions; however, these could be added in future to complement news articles.

Only four incidents and hazards concerning consumer products in the UK specifically have been reported in the media between December 2017 and June 2024, i.e. a period covering more than six years, and logged on AIM (OECD, 2024a). Similar figures, or indeed no incidents, were observed in other countries. Considering the results more closely, it appears that the **term consumer product has been interpreted in a broad manner**, reflecting not only products that have AI incorporated but also the wider impact of AI on consumer product markets. For example, there is an article about a generative AI programme creating the most beautiful man and woman in the UK for a health and beauty company (OECD, 2024b). The story is categorised under the human rights harm type, with the affected stakeholders listed as the general public and women. As well as consumer products, the story is categorised under: arts, entertainment and recreation; media, social platforms, marketing; and consumer services, since stories can cover multiple sectors (as well as the OECD AI Principles).

Other examples focus on the use of facial recognition in cameras by UK retailers to identify suspected criminals. The technology scans shoppers' faces, checks them against a database and sends an alert to the shop should a match be identified. According to the story, images of subjects of interest are stored for a year, unless the suspect is assumed to have reoffended, while images of all other people are deleted. It is listed under the human rights harm type, under the AI principles privacy and data governance, respect of human rights, robustness and digital security, and safety. A privacy campaign group has issued a legal challenge with the Information Commissioner's Office (ICO), alleging that the system breaches data protection laws due to the disproportionate balance between information processing and the need for crime prevention. Further, the cameras have been listed as a national security threat in the US, while the UK Government advised against the use of the company's equipment (OECD, 2024c).

One news story from December 2017 reports on the misuse of internet bots using AI to order multiple items and resell them at higher prices. Watchdogs have blamed them for shortages of toys, while coders are alleged to be behind the use of these bots and scalper software. The story is categorised under the economic/property harm type (OECD, 2024d).

The incidents and hazards covered under the consumer products category are **varied and wide-ranging**, with none related to any of the products covered earlier in this report (e.g. household items). Indeed, wider research found that the **threats resulting from the integration of AI in these consumer products are mainly potential in nature**. For example, considering smart glasses and wearables more generally, concerns around data privacy, recording and social engineering (the user unknowingly granting access to information) persist, but tend to be more abstract (Barge, 2024). These devices contain features to mitigate security risks, as previously outlined (such as muting the microphone on a smart speaker, or simply turning smart glasses off). Similarly, there have been concerns around the provision of updates in smart domestic appliances ending before their average lifespan, leading to loss of functionality. However, these are considered potential harms (Martin, 2023). Using the previously mentioned example of LLMs offering opinions and providing information, there have been well-known cases of AI tools providing **erratic, inaccurate answers** (McMahon and Kleinman, 2024). However, it ought to be highlighted that **many answers provided by AI tools are accurate**, though there remains a need to verify outputs (University of Maryland, 2024).

Clearly, it is quite possible that more harms have occurred due to the use of AI in consumer products. Conversely, it is possible that fewer harms have occurred due to the use of AI in consumer products and its safety benefits. It ought to be recalled, however, that AIM only covers reputable news outlets with, as yet, no option for open submissions of incidents, court judgements or decisions made by authorities. To put the number of incidents and hazards into context, the database reports on 11,536 hazards and incidents across all industries and countries. Under the consumer products category specifically, 167 have been reported. The number of incidents and hazards specific to the UK, at least those reported in the media, can therefore be **considered to be minimal**, shedding light on the scale of harms resulting from the use of AI in consumer products.

At present, the evidence base for making judgments on the scale of harms caused by the integration of AI into consumer products is not as extensive as it should be in future. However, based on current evidence, it would appear that the potential for harms, and the scale of theoretical harms, as detailed in this report and the previous study, are **greater than the actual harms**. The nature of the harms, whether theoretical or actual, highlight the importance of reporting and monitoring incidents and hazards.

5. Regulatory considerations

This section considers the current regulatory framework for product safety in light of the use of AI consumer products, focusing on any relevant changes since the previous study. In particular, it covers the regulatory and policy developments that have occurred in the intervening years and their appropriateness to mitigating emerging challenges. A summary of the findings from the 2021 study has been provided below.

For **many AI consumer products, the regulatory framework for product safety and liability, and the mechanisms in place to monitor product safety, are applicable and sufficient**. However, more complex AI systems and general technological trends pose challenges across the regulatory regime. General technological trends include: the blurring of the lines between products and services; the ability to cause immaterial and material harm; the increasing complexity of supply chains for consumer products; and issues related to obsolesce and maintenance during a product's lifestyle. These can challenge product safety and liability-related legislation, as well as market surveillance, standardisation, accreditation and conformity assessment systems.

The characteristics of AI systems, the general trends highlighted, and the lack of clarity around the applicability of existing legal definitions and concepts, bring additional impacts. These include a lack of legal certainty for economic operators involved in the manufacture of AI-driven consumer products, as well as a need to improve the skills and knowledge of regulatory bodies, such as market surveillance authorities (MSAs) and conformity assessment bodies, on AI systems.

Regulatory and policy developments

There have been a number of regulatory and policy developments in the field of AI in recent years, both in the UK and further afield. For example, section 4 considered efforts by the OECD in support of a reporting framework and monitoring system on different types of harm from the use of AI.

One key UK regulatory development is the **Product Security and Telecommunications Infrastructure Act 2022 (PSTI Act)**, and the associated Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023. There are two main parts to the Act which set out the duties. Part 1 sets out security requirements for consumer connectable products (including AI consumer products) to boost security against cyberattacks. Part 2 focuses on the deployment and expansion of mobile, full fibre and gigabit-cable networks across the UK (facilitating the use of connectible products).

The UK's new consumer connectable product security regime places obligations on manufacturers, importers and distributors of these products. Although the specific requirements vary according to the entity's role, broadly they need to: comply with minimum baseline security requirements (including minimum password requirements, the provision of information on the minimum period during which security updates are provided, and the provision of information on how to report security issues); the statement of compliance; investigating and remedying any suspected compliance failures; maintaining records of investigations and compliance failures; notification requirements of compliance; and taking action to prevent non-compliant products entering the UK market.

Breaches can lead to sanctions, including product recalls and fines of up to GBP 10 million or 4% of worldwide revenue.

Although previous legislation in the form of the **Consumer Protection Act 1987** and **General Product Safety Regulations 2005** set out a framework for product safety, it excludes minimum security requirements and was not suited to the connected nature of modern products. The new regime, which came into effect in April 2024, recognises the proliferation of consumer connectable products on the UK market, the potential security challenges and resultant harms, and mitigation measures.

Other major developments in the UK include: (i) the launch of the **AI Safety Institute (AISI)**, which is the first of its kind and is tasked with testing the safety of emerging types of advanced AI; and (ii) DSIT's **AI white paper** (2023). The white paper presents an approach to AI regulation that is principles-based and supports responsible innovation. It does not seek to appoint an AI regulator, instead adopting a cross-sector, context-specific approach, empowering existing regulators to develop tailored approaches that suit the way AI is actually being used in their sectors. In this respect, it differs from the centralised approach to regulating AI taken by the EU through the AI Act, as discussed below.

The principles were initially introduced on a non-statutory basis to avoid hindering innovation and reducing the UK's ability to respond quickly and proportionately to new technological developments. It had been anticipated that statutory regulations would be introduced in future if considered valuable and, also, if parliamentary time allowed. LLMs are included in DSIT's approach to AI regulation. The five principles regulators should consider to enable the safe and innovative use of AI are:

- **Safety, security and robustness**: AI systems should function in a robust, secure and safe way throughout the AI life cycle. Regulators may need to introduce measures for regulated entities to ensure their AI systems are technically secure.
- **Appropriate transparency and explainability**: AI systems should be appropriately transparent and explainable. Parties should have access to the decision-making processes of an AI system, increasing public trust.
- **Fairness**: AI systems should not undermine the rights of individuals and organisations, discriminate unfairly or create unfair outcomes.
- **Accountability and governance**: AI systems should be subject to governance measures ensuring effective oversight, with clear lines of accountability in place.
- **Contestability and redress**: Where appropriate, users, impacted third parties and actors in the AI life cycle should be able to contest an AI decision or outcome that is harmful or creates material risk of harm. Regulators will be expected to clarify the methods available to contest AI decisions and receive redress.

These principles strongly reflect the categorisation of AI challenges discussed in the 2021 scoping study and reiterated in section 4.

At present, the **principles-based approach offers flexibility in how AI is used**, including in consumer products, with the aim of supporting innovation in a field which continues to develop at a fast pace. The UK's approach to date contrasts with that of the EU, which enacted the rule-based **AI Act** in August 2024. While the UK's approach to regulating AI differs from the EU's, the core objective for both the UK and EU is maintaining safety while promoting innovation. Considered to be the world's first comprehensive AI law, the AI Act sets out harmonised rules on the development, marketing and use of AI across the EU. The law seeks to ensure that AI systems are safe and respect fundamental rights and values, while fostering investment and innovation, enhancing governance and enforcement, and supporting a single market for AI (EU, 2024).

The legislation prohibits AI systems posing unacceptable risks which are considered a threat to people. These include: cognitive behavioural manipulation of people or specific vulnerable groups (such as voice-activated toys that encourage dangerous behaviour in children); social scoring; biometric identification and categorisation of people; and real-time and remote biometric identification systems (such as facial recognition). High-risk AI systems are those affecting safety or fundamental rights, and will need to be assessed before being put on the market and also throughout their lifecycle. Limited risk AI systems include those with a risk of manipulation or deceit. These must be transparent, with developers and deployers ensuring that end-users are aware they are interacting with AI (e.g. chatbots and deepfakes). Minimal or no risk AI systems include applications such as AI-enabled video games or spam filters. These face no obligations, but companies can commit to voluntary codes of conduct.

If the AI system is the safety element of a product or the AI system is a product covered by EU product safety legislation and those products are required to undergo a third-party conformity assessment, then they will be deemed as high risk. For example, products which incorporate predictive maintenance would undergo such an assessment, which intends to offer increased levels of product safety when products are placed on the market. It is a blanket rule that does not necessarily consider the specific elements of AI consumer products where a second-party conformity assessment or even a self-declaration would suffice. Further, as outlined, the mutability of AI consumer products could pose problems after being placed on the market. If the product changes substantially, the conformity assessment originally undertaken could become redundant. Additionally, companies may be unwilling to bear the cost of an assessment, with the risk that such a rule could stifle innovation. However, safety is the key feature and other markets outside the EU could benefit. If a particular product is permitted within the EU having undergone a conformity assessment and is then placed in another market, consumers may have greater confidence that the product is safe. The balance between safety and innovation is certainly an interesting dynamic.

The EU's **General Product Safety Regulation (GPSR)** also impacts products that contain AI. The law, which applies from December 2024, stipulates that entities other than the manufacturer that substantially modify a product will be considered as 'manufacturers'. The GPSR refers to software updates and notes that these can substantially change the original product and impact its safety.

The UK government has indicated it will introduce legislation to specifically regulate the developers of the most powerful AI models, without formal commitment to general AI regulation. Currently, consumer product liability issues in the UK are regulated by the aforementioned Consumer Protection Act. The previous study detailed the product liability issues associated with the incorporation of AI into consumer products, including key technical characteristics which present a challenge for the liability regime. The changing nature of these products, which are becoming increasingly complex as they integrate new technologies, and new actors in the value chain, such as software providers, are **challenging liability rules**. As such, it is unclear to what extent the manufacturer should be held liable if damages could not have been predicted and are a result of software upgrades and updates, or alteration through interaction with consumers and their data.

In a liability regime, where the burden of proof lies with the claimant, a changing product could present a challenge for proving malfunction and damage, the attribution of liability, and claiming compensation. It is difficult to determine the extent to which the changing nature of AI consumer products currently presents a real threat to UK consumers as, to date, there have been few reported cases of AI consumer product liability being treated by UK courts. However, it is possible that the demand for clearer liability rules will become stronger as AI technology evolves and the risks become more clearly understood.

Related to the issue of liability, AI consumer products changing during their lifetime could present product safety challenges. Products that may have been safe prior to placement on the market could cause harms after software updates or through outputs derived from the increasing amounts of data used by algorithms, potentially burdening regulators to monitor and remedy product safety risks. However, there are measures that could be taken to limit the possibility of harms being caused by AI consumer products. These include: data quality assurance; encouraging increased transparency from companies in product/algorithmic design; post-algorithmic checks; and facilitating the self-reporting of harms experienced by consumers. While these measures may be burdensome, they would attempt to increase the safety levels of AI consumer products after being placed on the market. However, it ought to be recalled that the potential harms remain greater than the actual harms, with limited evidence of actual harms identified.

Singapore and **Japan** are taking a similar approach to the UK, with no specific laws, rules or regulations directly regulating AI. In Singapore, the government has issued various frameworks to foster innovation in AI while promoting its responsible use. AI Verify, an AI governance testing framework and toolkit helps organisations to test their AI systems against a number of AI ethics principles. It was developed by the Infocomm Media Development Authority of Singapore (IMDA) and the private sector (IMDA, 2022). More recently, the AI Verify Foundation and IMDA have developed the Model AI Governance Framework for Generative AI, which provides guidance on suggested practices to ensure the safety of generative AI models (AI Verify Foundation and IMDA, 2024).

In 2024, the Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) in Japan published AI Guidelines for Business Version 1.0 (MIC and METI, 2024). Though not legally binding, the guidelines are expected to promote compliance with AI principles and a risk-based approach among developers, providers and business users of AI systems. A proposed law for AI, called the Basic Act on the Advancement of Responsible AI, aims to regulate certain generative AI models. The law would enable the government to designate the AI systems and developers that are subject to regulation, imposing certain obligations on them. If passed, the law would signify a hard law approach to AI regulation in Japan. Further, under Japan's presidency of the G7 in May 2023, the Hiroshima Process International Guiding Principles for Organisations Developing Advanced AI Systems was launched (G7, 2023). These aim to promote safe, secure, and trustworthy AI worldwide, and provide guidance to organisations developing and using the most advanced AI systems.

The US is taking, to an extent, a different direction to Europe, considering how current regulations apply to AI. Lawmakers are undertaking a broad review of AI which seeks to balance its benefits against its harms, helping them to understand which specific aspects of AI could be regulated. However, a **stronger stance has been taken towards the most powerful foundation models**. At the end of 2023, the White House issued an executive order requiring companies that create powerful, dual-use systems to disclose system capabilities, while promoting guidelines, standards and best practices to help ensure the development of safe, secure, and trustworthy AI systems. It was the first comprehensive effort to address AI in the US (The White House, 2023). In May 2024, Colorado became the first state to pass a law addressing the use of AI in employment and other fields

(Colorado General Assembly, 2024). In China, meanwhile, a law designed to regulate generative AI entered into force in August 2023 (Cyberspace Administration of China, 2023), while a draft AI law focusing on industry development was published in March 2024 (Costigan, 2024). In **South Korea**, the National Assembly has passed legislation to enact the Act on Promotion of the AI Industry and Framework for Establishing Trustworthy AI (National Assembly of the Republic of Korea, 2023). This is expected to become a consolidated body of law, incorporating several AI-related bills introduced since 2022. The purpose of the Act is not only to promote the industry but also protect users by developing a more secure ecosystem that puts in place stringent notice and certification obligations.

In summary, a **number of regulatory and policy developments have taken place** since the previous study was undertaken, demonstrating the increasing opportunities, and potential threats, posed by AI. Businesses, too, aim to ensure product safety throughout the product's lifecycle; however, there is a lack of publicly available data on the mechanisms implemented and steps taken by businesses in this regard.

However, as outlined, it would appear that the potential for harms, and the scale of theoretical harms, remain **greater than the actual harms**. With AI having become more prevalent in consumer products since the previous study, and this trend set to continue, it is critical to monitor developments to understand whether the status quo changes.

6. Conclusions and future considerations

This section presents the conclusions of the research, and provides some strategic considerations for OPSS in responding to any potential challenges arising from AI consumer products.

AI techniques and systems are constantly evolving; it is therefore important to assess how different parties **understand and define AI** both as a general purpose technology, but also the variety of applications, techniques and systems that fit within the AI umbrella, including consumer product applications. In this context, significant work has been done since the 2021 OPSS study to further explain AI in specific contexts.

From a technical perspective, the most prominent development in this regard since the 2021 study is the **widespread adoption and use of frontier AI models**, including large language models (LLMs), such as GPT-4. These models have enabled advances on the path towards artificial general intelligence, but also advances in the performance of narrow AI models in certain contexts (e.g. generative image models). Moreover, emerging concepts illustrate the increasing focus on identifying and tackling the risks and challenges associated with AI (e.g. emergence of the field of AI safety, or the term hallucination to describe how AI chatbots can confidently present false information).

Considering the **regulatory landscape**, many stakeholders have outlined their understanding of AI and its regulatory implications, including the UK Government, the EU and the OECD. The definitions put forward by these authorities generally highlight similar capabilities and characteristics; namely, the ability of AI systems to: (i) infer how to generate outputs based on the inputs they receive; (ii) adapt their operations based on 'training' such that the outputs and outcomes are not easily interpreted and/or not directly envisioned by humans; and (iii) act and take decisions autonomously.

However, while the specific situation of AI in consumer products continues to receive limited focus, it can be concluded that the developments since 2021 are largely in line with the findings from the 2021 OPSS study on the key characteristics of AI and how they can lead to different risks and challenges in consumer products.

The **market for smart connected home devices remains strong**, having grown by a third since 2017-2018, with an increasing number of adults owning a connected home device, up 14% since the previous study. New products have emerged on the market, including smart wearables and AI-enabled assistance robots, while generative AI, a major development in the field of AI since the previous study, is set to transform AI consumer products (Hafke, 2024).

One key challenge, which remains from the previous study, is determining the exact scale and size of the AI consumer product market. Market data does not tend to differentiate between AI and non-AI connected home devices, often referring to both categories as smart products. As such, a closer examination of the individual smart product categories is required to understand whether AI is integrated. Such an approach can help to distinguish between AI and non-AI consumer products, though it has its limitations since some product categories contain both types of products, and the data does not offer an overarching view of the market. While data indicates a growing smart product market that contains a significant number of AI-enabled products such as smart speakers, washing machines and refrigerators, **ownership levels of smart products among the wider population remain relatively low**, aside from smart TVs and smart speakers. Although future market predictions refer to smart products, the limited overarching market data on AI-enabled products specifically should not be considered as a reflection of the maturity of the market overall. Indeed, the market for AI consumer products itself is only likely to grow, in line with the wider, global AI market.

The monitoring of market developments is important to understand the market better, the products driving the market and the typical uses of AI, which can better inform product safety regulation. It should be noted that the AI consumer product driving the market remains the smart speaker. Further, although there are more products using AI on the market now than previously, the current size of the market should not be overestimated given low ownership levels. These market dynamics should be taken into account when considering if further regulatory action is required. For now, at least from a market perspective, there would not appear to be any significant risks posed, in a similar vein to the previous study.

AI consumer products offer a number of benefits, but also challenges and risks. However, **these remain essentially the same in nature** as those detailed in the previous study. The benefits include convenience, efficiency, enhanced personalisation and security. Predictive maintenance monitors the health and performance of devices in real-time, allowing organisations to forecast the performance status of components to ensure a repair can be scheduled. This feature therefore plays an important role in preventing accidents from occurring. Devices also contain security features, enabling consumers to exert control over their data and content and enhance their privacy.

The key characteristics of AI systems (mutability, opacity, data needs and autonomy) can lead to **material or immaterial harm**. Since the previous study, further work has been undertaken to provide a better understanding of AI harms and the types of harm. At the OECD level, for instance, an AI incident reporting framework is being developed, along with the monitoring tool AIM, which has led to increased awareness among stakeholders of the risks posed by AI systems, including those in consumer products. However, the approach to reporting harms remains in development, suggesting further research is required and reflecting the relatively new nature of AI-related harms, ongoing discussions about risk mitigation and the relative scale of the harms. Indeed, the **research identified limited evidence of actual harms**, and the potential harms remain greater than the actual harms.

From a product safety perspective, this finding is positive and, while AI technologies have evolved since the previous study, the resulting threats have not become significantly greater in scale. However, it is unclear whether, how and when **the potential harms could increasingly become actual harms**, given the speed at which new AI technologies are created. Moreover, limited information exists on the steps taken by manufacturers to examine, characterise and address the specific risks of harms related to the integration of AI systems in consumer products.

The UK, as a member of the OECD, should continue to play a key role in the development of the incident reporting framework and could even consider implementing its own system to allow consumers and businesses the opportunity to report incidents. Such a move would potentially capture incidents that have not been reported elsewhere, would improve understanding of the harms that occur, and facilitate appropriate responses to be taken. Furthermore, direct engagement with manufacturers, as well as testing, certification and conformity assessment stakeholders, for instance through a targeted research project, could be conducted to provide more detailed insights into the perceptions of the risks in specific products and the steps taken by manufacturers to address those risks.

A number of regulatory and policy developments have taken place since the previous study. As AI technologies evolve, further consideration is given to the best way to ensure AI systems remain safe, secure and trustworthy while fostering innovation, with different approaches taken. Certain jurisdictions, including the UK, US, Singapore and Japan, **currently approach AI regulation, generally, in a non-statutory manner**, with various guidelines and toolkits developed with industry to promote the development and testing of AI systems while fostering their safety, particularly generative AI models. This soft law approach has been taken to restrict rules imposed on companies, while encouraging innovation and the responsible use of AI systems in line with AI ethics principles. However, legislation has been mooted for the future in some jurisdictions, particularly towards the most powerful foundation models.

Other jurisdictions, including the EU, South Korea and China have **taken a stronger stance, introducing AI legislation**. For example, the EU AI Act prohibits AI systems that pose unacceptable risks, while high-risk and limited risk systems face certain obligations. Legislation can improve product safety, with requirements such as third-party conformity assessments in place. However, there is a risk that stringent rules stifle innovation, while developments in the field of AI could necessitate changes in rules in the near future. Yet, with the global nature of trade, product checks in one jurisdiction could benefit consumers of those products in others, improving their confidence in product safety. Equally, proponents of a hard law approach might suggest that guidelines insufficiently treat the safety and responsible use of AI systems, offering less consumer protection.

Clearly, there are merits to both approaches. Product safety regulators should be encouraged to monitor the use of soft law measures, as well as the application of legislation, before determining which next steps ought to be taken. Different jurisdictions are considering introducing legislation to regulate the most powerful foundation models, should there be reasonable justification. Countries and international organisations should continue their collaboration, monitor developments and engage with various stakeholders, including consumers, industry, government agencies, academics and researchers, product safety practitioners and standards bodies. These actions could lead to a shared understanding of AI, related harms, the views of different groups and guidance on the actions to be taken moving forward, while giving individual jurisdictions sufficient flexibility in their approach to AI regulation.

Annex 1: Case studies

This annex presents four case studies that aim to examine the following topics related to AI and consumer products in more depth:

- Concept of generative AI, its use in consumer products and implications for product safety.
- Hazards resulting from the integration of AI in consumer products.
- Smart glasses – the role of AI and the related opportunities and risks.
- AI and robotics – the role of AI and the related opportunities and risks.

The selection of case studies was conducted in collaboration with OPSS.

Generative AI

Generative Artificial Intelligence (AI) refers to a class of deep-learning models capable of producing high-quality content—such as text, images, or audio—based on patterns and data they have been trained on. These models can take vast amounts of raw data and generate statistically probable outputs when prompted (Martineau, 2023). The release of OpenAI's ChatGPT marked a significant milestone in popularizing this technology, showcasing its ability to perform diverse tasks by learning from large datasets and adapting through fine-tuning. In particular, with the emergence of foundation models, generative AI systems can now be trained on massive volumes of unlabelled data to produce representations that generalize well across multiple tasks, making them adaptable to a wide range of applications.

The integration of generative AI into consumer products has ushered in a new era of personalised, interactive experiences. From voice-activated toys and assistants in smart speakers to advanced writing tools and content creation software, the impact of this technology is becoming increasingly widespread. Consumer-facing applications, such as Adobe Photoshop, leverage generative AI to enhance creativity, while health-related devices like the OURA ring utilize AI for data-driven insights into personal well-being. Additionally, AI-driven chat assistants have gained prominence, offering personalised customer service, product recommendations, and even mental health support through apps. This case study aims to explore the growing role of generative AI in consumer products and assess the opportunities, risks, and considerations that arise.

Toys are becoming increasingly integrated with generative AI. In 2023, the musician Grimes and the company Curio developed an interactive AI plush toy in partnership with OpenAI that can converse with children and learn their personalities, with three characters created. The toys can provide parents with a transcript of conversations. The company stated that the toys do not store voice data, while the transcripts are stored in compliance with the Children’s Online Privacy Protection Act. Transcripts are deleted after 90 days (Khalid, 2023).

Smart rings have emerged as a popular category of wearable technology, offering users advanced health and fitness tracking in a compact form. In 2023, smart rings generated USD 210 million in revenue, and forecasts from Global Market Insights predict that the market will expand at an annual growth rate of 24.1%, reaching USD 1 billion by 2032 (Bajarin, 2024). Among these devices, the Oura Ring stands out as a leading product, known for its comprehensive health- and sleep-tracking capabilities. It monitors key metrics such as heart-rate variability (HRV), blood oxygen levels, body temperature, and sleep duration, providing users with detailed insights into their overall well-being (Lemire, 2024).

With over 2.5 million units sold worldwide (Oura, 2024), the Oura Ring reflects the growing demand for smart health devices. Oura has recently introduced a generative AI-powered feature, Oura Advisor, designed to enhance the user experience through personalised health insights and recommendations. The generative AI, integrated within the Oura app, acts as a 24/7 virtual health coach (Lemire, 2024). The AI-powered chatbot answers user questions, learns about individual habits, and provides tailored advice based on the user's specific needs, such as fitness goals or personal circumstances. The system is built on a large language model (LLM), though Oura has not disclosed the exact model used.

Competitor products like Whoop's fitness tracker have developed similar AI features, such as the Whoop Coach, using ChatGPT (Lemire, 2024). Generative AI models like the one powering Oura Advisor use deep learning to analyse vast amounts of data. The algorithms analyse the connections between words and build a probability model based on these relationships. When given a ‘prompt’, the algorithm generates a response by predicting the most likely sequence of words according to its learned patterns (National Cyber Security Centre, 2023).

Several concerns and challenges surround the use of generative AI in consumer products like the Oura Ring. One major issue is that the Oura Ring’s LLM stores user details in a manner that influences the evolving guidance provided. This personalised “memory” accumulation allows for increasingly tailored recommendations, but it also means that sensitive health data, such as menstruation cycles or recovery statuses, could potentially be used in future AI model development (Krol, 2024).

While the Oura Advisor feature is opt-in (users must consent to having their personal health data analysed to receive personalised recommendations and ‘memories’ can be deleted) (Krol, 2024), the storage and use of such sensitive information raise concerns about data security and the risk of harm of fundamental privacy rights, particularly from a cybersecurity perspective. The use of generative AI introduces risks associated with data breaches and hacking. Although Oura is a private company and its AI is not a public LLM, it still invites concerns about the vulnerability of sensitive health information being leaked. The National Cyber Security Centre (NCSC) advises against submitting sensitive data to public AI systems (National Cyber Security Centre, 2023), and similar caution may apply here, even though the Oura AI operates within a more controlled environment.

Further concerns include the limitations inherent in LLMs themselves. These models can be prone to errors, including “hallucinations,” where they generate incorrect or misleading information (National Cyber Security Centre, 2023). In the context of health devices, this can lead to significant safety risks. A recent study showed that a portion of LLM-generated medical advice contained safety errors, and in one instance, the advice was dangerously incorrect (Chen et al., 2024). However, no specific studies have been conducted on the AI systems employed by Oura or similar smart devices. Despite these challenges, generative AI holds significant potential in enhancing consumer products. For example, in the context of fitness and health tracking, the ability of AI to process vast amounts of user-specific data can provide highly personalised insights that were previously unavailable. While further work is needed to ensure the accuracy and safety of the advice provided, AI-based systems offer consumers more precise and tailored information on their fitness and health, enabling proactive management of their well-being.

Hazards resulting from the use of AI in consumer products

Issues of consumer product safety, data security and privacy have traditionally been dealt with by separate regulatory authorities, while product safety risk assessments typically focus on physical harm to people. However, products integrating new and emerging technologies, including AI, are challenging traditional product safety regulatory environments. Traditional product safety risks converge with cyber security and data protection concerns in these more technologically advanced consumer products, which can also enhance the risks of psychological and economic harms.

In this context, this case study broadly explores the application of existing product safety concepts to the specific applications of AI in consumer products by: (i) presenting an overview of relevant concepts; and (ii) isolating the mechanisms by which AI systems could lead to different types of hazards from consumer products.

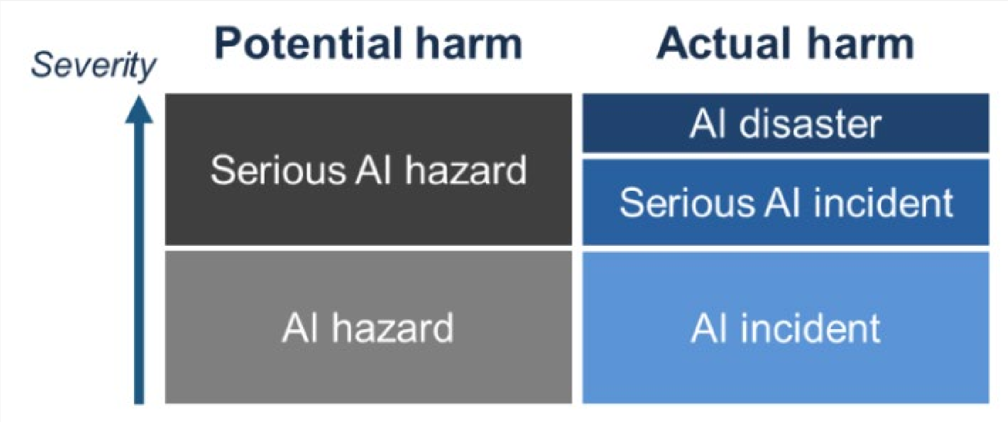
Overview of existing concepts

The Product Safety Risk Assessment Methodology (PRISM) framework and supporting lexicon (OPSS, 2022; OPSS, 2021) outline various different elements that need to be considered and examined when assessing the safety risks stemming from a product. Key risk-related terms include:

- **Hazard**: A potential source of harm, the level of which should be determined by the nature of the harm it can cause if realised (in terms of severity) and the anticipated extent of that harm (in terms of the number of people that could be affected).
- **Harm**: Adverse impact on individuals, the environment, infrastructure property, animals, or businesses, and which can include human injury and ill health, damage (including disruptions) to property, damage to the environment, or economic loss. In line with the scope of this project, this definition is broad in nature, encompassing adverse physical, mental, social and economic impacts.
- **Risk**: A function of the level of a hazard and the likelihood that the hazard will cause harm.

Furthermore, the OECD framework for defining AI incidents and related terms (OECD, 2024), cited in the main body of this report, presents a proposed classification for AI risks based on the severity of the risk and whether the harm is potential or has actually been experienced (see below figure). In this context, the OECD framework provides draft definitions for an ‘AI hazard’ and a ‘serious AI hazard’.

While the main body of this report examines the potential challenges and harms stemming from AI consumer products and these frameworks establish a basis for understanding general and general-AI hazards, neither framework assesses the specific hazards resulting from the use of AI in consumer products.



This diagram illustrates how the categories of potential and actual harm change based on level of severity. As severity increases, potential harms develop from AI hazards to serious AI hazards, while actual harms develop from AI incidents to serious AI incidents to AI disasters.

Specific hazards of AI consumer products

In this context, it is also important to recognise that each consumer product has a body of risks that stem from its specific product characteristics, functions and components. For instance, these might include physical hazards stemming from the design of the physical product, such as the presence of small parts with the potential to be inhaled or ingested, or from the connected nature of a product, such as a loss of connectivity leading to hazards (e.g. electrical overload due to the inability to turn off a connected oven).

As such, isolating the role of AI systems in these complex products is challenging and requires a focus on the core characteristics and related challenges of AI-driven consumer products that differentiate them from consumer IoT / connected / smart products, as well as traditional consumer products. In summary, these characteristics include mutability or adaptiveness; opacity; data needs; and autonomy. As per the 2021 study, the challenges that can result from these core characteristics are as follows. Here, we examine, in a non-exhaustive manner, the types of hazards that could stem from each type of challenge:

- **Robustness and predictability** – it is important for consumer products to perform as intended by the developer / manufacturer, and as expected by the consumer. Poor decisions or errors in the design and development of an AI system used in a consumer product could lead to unintended, poor algorithmic and thus poor product performance. In theory, challenges in this field are the core mechanisms through which physical hazards can exist as a result of AI in consumer products. Furthermore, as AI can be used in such products to control and inform any functions and components, challenges in this context could result in mechanical, electrical, thermal and other physical hazards. For instance, the use of poor training data could result in distributional shift (e.g. a cleaning robot might be trained and optimised for cleaning one environment, such as a room without open stairs; as a result, the robot may not operate in a safe way when deployed in a context with open stairs). Additionally, the provision of inaccurate information could put consumers in dangerous situations.

- **Transparency and explainability** – many AI systems, particularly more complex models, lack transparency and explainability due to the choices of developers, who may be required to accept trade-offs between performance and transparency. While challenges in this area may not translate directly into hazards, they can have an impact on consumers, who may not be aware of AI being used within products. These challenges can also have implications in a product liability context, as even the developers, let alone the consumer or regulatory authorities, may not be able to understand and explain why something has gone wrong as a result of errors, poor design or malfunctioning of an AI system.
- **Security and resilience** – the use of AI in consumer product security functions is evolving, while the cyber security of connected consumer products is a prominent concern (as evidenced by the adoption of the PSTI Act 2022 and PSTI Regulations 2023). Issues with AI-driven security functions, including poor design, malfunction, or manipulation by malicious actors, could lead to secondary physical and psychological hazards. For instance, a malicious actor could manipulate a smart oven to turn on while the owner is out of the house, without warning the owner leading to possible thermal, fire or electrical hazards. In addition, while also a key challenge for connected products generally, a loss of connectivity or challenges with interoperability and integration between different products and devices could lead to reduced functionalities.
- **Fairness and discrimination** – many examples of AI systems producing discriminatory results have been found. Challenges in this context can result from biases or imbalances in the data used to train, validate and test such systems, or in the methods and mechanisms used to categorise and classify data (Crawford, 2013). While it is not clear how challenges in this area could lead to physical hazards, they could cause immaterial harm by reducing accessibility and accuracy of outcomes.
- **Privacy and data protection** – given the data-driven nature of AI systems, privacy and data protection challenges can emerge. Again, it is unclear how these challenges could lead to physical hazards. However, AI systems can transform non-sensitive data into sensitive personal data, learn and take automated decisions on that basis, which could also lead to unfair or discriminatory outcomes as highlighted above. Furthermore, security issues could lead to personal data breaches and related psychological or mental health impacts.

Given the lack of specific incidents and the limited publicly available information on how manufacturers examine and address AI-related risks, it is challenging to examine how these hazards have evolved since 2021 or might evolve further in future. In this context, while the above general typology of the risks and hazards is not anticipated to change, it is important to note that the nature of the hazards and risks are specific to the type of products and the way in which AI is integrated into each product; some may bring only minor risks, while others may introduce more significant risks, with varied profiles of risks across the types of challenges highlighted above. In this context, as the types and number of consumer products that integrate AI in some way increases, there will need to be a greater focus on assessing and tackling AI-related product safety risks.

Smart glasses

While the concept of smart glasses has been around for decades, the incorporation of AI into this consumer product is a relatively recent development. With the potential to offer various functionalities with the use of AI, smart glasses are becoming increasingly popular among consumers.

While traditional functions of smart glasses included displaying information, images, and taking pictures, AI can enhance their capabilities, making them more intuitive and personalised. For example, generative AI can augment image recognition, enabling smart glasses to identify and describe objects, providing information in real time (Ambiq, 2024). AI-enabled voice controls facilitate hands-free user interaction with their smart glasses, enabling calling, messaging, recording videos and obtaining information (Meta, 2024b). Smart glasses can also utilise natural language processing (NLP) to enhance the user experience, allowing smart glasses to understand and respond to natural language commands (Ambiq, 2024). For example, users can ask for translations of foreign signs, or request captions to images, with the functionalities set to grow in future (Meta, 2024a). This use of multimodal AI, i.e. the ability for AI to process multiple types of information such as images, audio and text, is a major feature of smart glasses and a significant step to enhancing user experience.

In addition to the features mentioned above, AI-enabled smart glasses have the potential to benefit individuals with low or no vision, assisting them with daily chores. As well as helping with tasks such as navigating rooms, finding objects and recognising text for reading, the voice command feature can assist individuals with advanced functions, such as searching for restaurants. Smart glasses can even provide additional information, such as reviews, menus and prices. Sensors play an important role, enabling the AI smart glasses to perceive and understand the surrounding environment. These include cameras, microphones, gyroscopes and accelerometers (Pal, 2023).

Although AI smart glasses can offer a number of benefits, as outlined above, they also have the potential to cause risks and harms, with concerns around privacy, security, health, social implications, and legal issues (Capsule Sight, 2023).

AI smart glasses with cameras and microphones enable users to record their surroundings discreetly, raising concerns about covert surveillance and privacy both for users and bystanders. Moreover, the use of facial recognition can present ethical challenges, with companies able to collect and profit from sensitive personal information. There are also potential security risks, whereby hackers exploit weak security measures to access sensitive data such as location information and passwords (Capsule Sight, 2023). AI smart glasses can also cause negative side effects. Unlike regular glasses that correct vision, AI smart glasses can cause vision and mental fatigue, as well as eye strain due to the close, prolonged proximity to displays. Further, blue light can cause insomnia and other sleep-related issues, while overdependence on smart glasses can reduce situational awareness, limiting an individual's ability to perceive and respond to the environment (Pal, 2023).

AI smart glasses could have a detrimental impact on social interactions, leading to less face-to-face communication and bringing about a sense of disconnection. Individuals may feel obliged to be constantly connected, exacerbating the "always-on" culture, while the digital divide could be further widened due to the cost of the latest product. From a legal perspective, regulations may become outdated with the technology's rapid development. It has been suggested that current and future legislation could limit the use of AI smart glasses in certain settings, while issues such as copyright infringement and harassment could arise, requiring clear guidelines and enforcement (Capsule Sight, 2023).

AI-enabled smart glasses have the potential to generate benefits for the user, as well as cause risks and harms. It ought to be pointed out that the use of AI smart glasses is not, as yet, common. As such, the potential risks and harms should be contextualised, relative to their actual usage. However, with smart glasses set to gain a bigger market presence, they should certainly not be underestimated and must be taken into account when considering the continued health and safety of consumers.

AI and robotics

Robotics and AI represent two different, but very related, fields of science and technology. While the field of robotics is concerned with the designing and building of machines capable of automating tasks, AI refers to machines developing the same intellectual capabilities as humans. Both robotics and AI aim to automate tasks and facilitate processes for individuals, using data collected by sensors to arrive at decisions. Robotics and AI can benefit from each other. Indeed, robotics is already utilising AI across a range of fields, such as healthcare, manufacturing and agriculture. Increasingly, robotics is utilising AI for consumer products, offering functions personalised to the user, for example to entertain or complete domestic chores.

Personalised robots offering companionship and healthcare functions have become increasingly prominent in recent years, incorporating AI to improve living conditions for individuals. One such example is ElliQ, which is specifically designed to address loneliness, empower independence and promote healthy living, particularly for the elderly (Intuition Robotics, n.d.). ElliQ uses voice, sounds, light and a touch screen to facilitate conversation, music, video calls, well-being assessments, stress reduction, cognitive games and health reminders. With the integration of generative AI into the latest generation of ElliQ, it now offers enhanced conversation with users. Information is understood, classified, remembered and later referenced in future conversations, ensuring that they remain contextual and relevant. Generative AI is also used to enable painting or writing poems, which can be shared with others, contributing to social well-being, decreased loneliness and a greater sense of recognition. Further, safety mechanisms have also been deployed to monitor and mediate conversations to avoid inappropriate responses and better control the context and flow of conversations (PR Newswire, 2024).

ElliQ is one example of a robot designed to improve the user’s daily life. Recently, the University of York’s Institute for Safe Autonomy developed a two-armed robot that can help an individual to get dressed. Adopting a method called learning from demonstration, a human demonstrates the required motion and the robot learns, without the need for it to be programmed. While human modelling can improve the efficiency and safety of human and robot interactions, it has been suggested that it is not only important that the robot performs the tasks but also that it can be stopped or changed mid-action at the request of the user. Indeed, trust plays an important role, with the next step being to test the robot’s safety limitations and whether it will be accepted by those most in need (Johnson, 2024).

One robot that has been developed for household and industrial chores is the EVE Android. Using a modified version of GPT-4, it can perform various tasks, including cooking, cleaning and suggesting recipes. Further, EVE Android can be used in an industrial setting. It can operate as a security guard, patrolling warehouses and alerting human operators when anomalies are identified, as well as undertaking tasks such as packing, sorting, printing, cleaning, and monitoring. It has been suggested that the widespread usage of robotic personal assistants, particularly for the elderly, will be possible within the next couple of decades, with the manufacturer taking a cautious and gradual approach to introducing the technology to wider society. Indeed, the importance of taking such an approach has been highlighted, enabling people to become familiar with robots and ensuring a smooth transition, with safety considerations taken into account (Kanana, 2024).

Other examples of robots designed to perform household tasks include: Tesla's Optimus, which has been seen picking up eggs, folding t-shirts and sorting coloured blocks; Dobb-E, which can put a sock into a washing machine and a potato into a microwave (and is trained by researchers performing tasks and being videoed); Dyson robots which can stack dishes, pick up objects and vacuum armchairs; and Sanctuary AI's Phoenix robot, which can already loads items into a bag, clean mirrors, sort objects and stock fridges, and is estimated to perform any human task within a decade (Waugh, 2024).

AI-enabled vacuum cleaners and lawn mowers have been on the market for some time, offering consumers convenience and saving them time. More recently, Electric Sheep Robotics have developed Verdie, a robot gardener which uses generative AI to help around the garden. Run on the company's ES1 model, it can create a bird's-eye view semantic map to facilitate travel over unpredictable terrain, and can also balance on two wheels. Verdie can be equipped with power tools and is able to strim lawn edges, or use a leaf blower or saw (Sansom, 2024). Many of the consumer products outlined here, like Verdie, are at the early stages of development but are expected to come to market, with the potential to offer users convenience, assistance, entertainment and satisfaction. However, it remains to be seen what future demand among consumers will look like, with adoption levels and wider public opinion set to play a significant role in determining their success.

Annex 2: Market for smart products

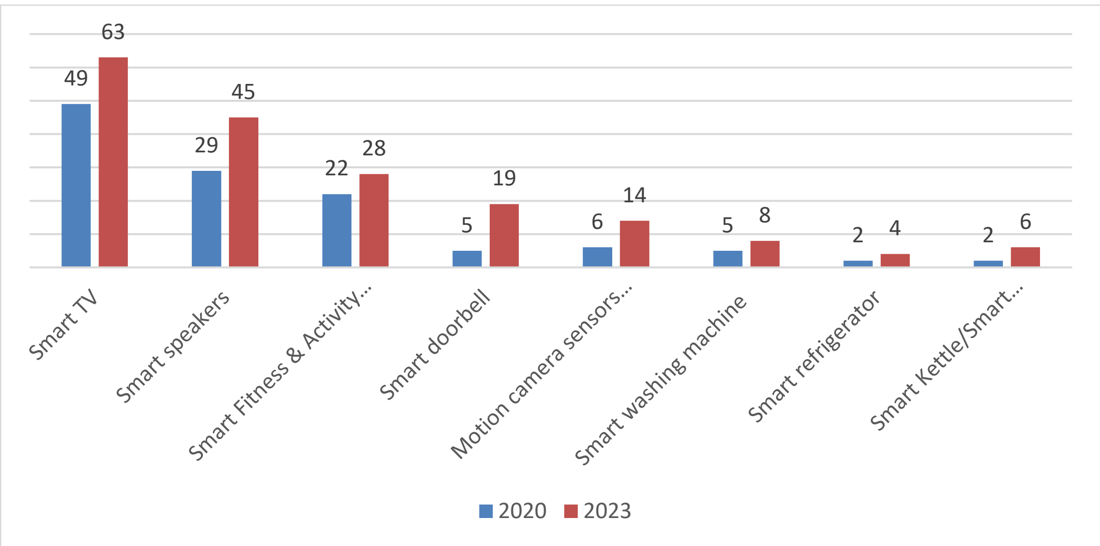
The market for AI consumer products continues to grow both in the UK and globally, as AI technologies evolve and more sophisticated products are placed on the market. However, the term AI continues to be conflated with other terms, most notably smart products. Therefore, **this analysis covers both AI and non-AI consumer products** (both categorised as smart products), as well as relatively advanced and simple uses of AI in consumer products. Examples of AI consumer products, including the types of AI used and their capabilities, are provided.

techuk's annual State of the Connected Home report categorises connected home devices under the following groups with specific product examples (techUK, 2023):

- **Smart Domestic Appliance**: Smart kettle/coffee makers; smart refrigerators; smart washing machines; and smart ovens/hobs.
- **Smart Entertainment**: Smart speakers (e.g. Google Home/Amazon Echo); and smart TVs.
- **Smart Energy & Lighting**: Smart thermostats; smart plugs; energy management services/apps; and smart lightings (smart lamps).
- **Smart Health Monitors**: Smart monitors for specific health conditions; smart fitness & activity trackers; smart connected scales; and smart connected toothbrushes.
- **Smart Security & Control**: Smart/connected alarm systems; motion camera sensors for external doors/windows; internal cameras for babies, pets or security; smart access controls (digital keys); smart doorbells; and smart detectors (for smoke and gas leaks).

Considering the UK market for smart and connected products, **80% of adults own at least one connected home device**, according to the report (techUK, 2023); this represents an increase of **14%** from the previous study. This figure is consistent with the proportion of the UK population familiar with the concept of a 'connected home', which is also 80%. The following table illustrates the changes in ownership levels of key smart products since 2021:

Figure 1: ownership percentage of key smart products in the UK



There has been an increase in ownership of all of these products. **Smart speakers continue to play a role in driving the UK smart home market**, with self-reported ownership at 45% in 2023, an increase from 29% in 2020 (techUK, 2023). Ownership of smart fitness & activity trackers has experienced a more moderate increase, while there have been significant changes in purchases of smart doorbells and motion camera sensors. AI-enabled domestic appliances such as smart washing machines and smart refrigerators are becoming more popular, with ownership levels having increased by 3 and 2 percentage points respectively since the previous study, though their current ownership levels remain low compared to other smart products, and below 10%. According to techUK's report, the share of those possessing more than three connected devices, referred to as 'advanced adopters', stands at 34%, double the figure from 2020 (techUK, 2023). However, this figure is over 40% for people aged 16-34 but only 22% for those over the age of 65, indicating that the significant growth since 2020 has come from the younger age groups.

Considering sales figures, 19,959,000 connected home devices were sold between April 2022 and March 2023, representing a small decline of around 2% from the previous year, when 20,400,000 units were sold. 58% (11,585,000) of the devices sold were smart TVs, wearables and printers, demonstrating the continued popularity of these categories, and smart TVs in particular, in the UK. The **smart entertainment category accounted for the highest proportion of sales volume** (41%), followed by health (18%), including wearables, and security & control (15%).In terms of sales value, the total for all connected home devices accounted for GBP 4.93 billion. The smart entertainment category experienced the highest proportion of sales value, at 58% (techUK, 2023). The sales volume and sales value figures **reflect a strong market for connected home devices** and, looking at previous figures from 2017-2018 (14,723,000 devices sold and GBP 3.38 billion in sales value), the market has grown by a third in this period.

While the most recent figures represent a slight decrease year-on-year compared to the period ending in March 2022 (by around 2% in sales volume and 3% in sales value from GBP 5.08 billion), they should be considered in the wider economic context. Specifically, sales of both connected and non-connected home devices under the same categories (domestic appliances, entertainment devices, energy and lighting systems, health monitors, and home security apparatus) have decreased by 7% in a year of generally poor economic performance (techUK, 2023).

High levels of inflation and increasing interest rates in recent years have reduced consumer purchasing power, with the lowest ever Consumer Confidence Index (CCI) score for British consumers recorded in September 2022. However, more positively, the national connected home market continues to surpass figures taken before the onset of the COVID-19 pandemic, reflecting continued interest and purchasing of smart devices and the resilience of the market (techUK, 2023).

In this context, it ought to be clarified that the **categories do not differentiate between AI and non-AI connected home devices**. Certain products under these categories, such as smart speakers, have AI incorporated and are designed to operate with some degree of autonomy based on data needs. Other products listed, however, are not AI-driven, such as smart thermostats and smart plugs. Smart TVs, which were traditionally operated without AI, are now incorporating AI to enhance viewer experience, from basic functionalities such as recommendations and noise reduction to more complex ones such as image isolation, contrast and tone enhancement, colour improvement and remastering old content. However, their presence on the market is far smaller in scale. Indeed, AI differs from automation. Whereas AI can adapt and operate with autonomy, automation refers to a device operating on basic, rules-based capabilities to replace repetitive manual and cognitive tasks carried out by humans.

The term smart device/product has long been used in marketing, encompassing both products which incorporate AI and those that may not. The wide range of products could explain why the term AI continues to be conflated with smart, which has become a marketing buzzword, implying that it will improve life for the user. Further, a smart device is a physical object that has been enhanced with technology (such as AI), whereas AI could be considered the ability to display autonomy and adaptiveness, which can be incorporated into products. International commodity codes refer to smart products or categorise devices under other headings and, with future market predictions using the term smart, and scope to further increase the incorporation of AI into consumer products, it is considered unlikely that the term will change in the near future.

As such, although the size and scale of the connected home devices market in the UK can be determined, the lack of data specifically on AI consumer products **presents a challenge in understanding the true size and scale of this market**. Indeed, the State of the Connected Home report notes: "We're excited to see which new product categories will emerge as smart home companies integrate artificial intelligence and machine learning into their devices, and how an increasingly well-informed and enthusiastic consumer base responds to these innovations". This demonstrates that, while AI products already have a strong presence on the market, **there remains scope to further increase their integration in consumer products and popularity** among consumers (techUK, 2023).

Market data from other sources also **indicates overall growth** in the smart product market. Data from Statista projects revenue in the UK smart home market to reach GBP 8.6 billion in 2024, with a forecasted Compound Annual Growth Rate (CAGR) of 9.4% between 2024 and 2028 (Statista, 2024a). Other sources of market research data also forecast growth in the global smart home market. These sources note that the growing trend of incorporating AI into consumer products is expected to increase demand, adding that **the COVID-19 pandemic acted as a catalyst in driving demand for smart products** (Grand View Research, 2023), while attributing future growth to a range of factors, including increasing consumer convenience and automation, security and surveillance, energy savings, ageing demographics and integration with mobile devices (The Business Research Company, 2024).Considering the sector more widely, the combined market valuation of the **UK AI sector** reportedly reached USD 92 billion (GBP 72.7 billion) during the first quarter of 2024 (Tech Nation, 2024). The value of UK AI has increased by 17 times since 2014, from USD 5.3 billion (GBP 4.2 billion), and by 2.2 times since 2019, from USD 41.6 billion (GBP 32.9 billion).

The figures cited above are consistent in illustrating the pace at which the smart home market, including AI consumer products, is set to grow. While the **available data does not allow for a quantitative assessment of the contribution of AI consumer products to this growth**, various sources have discussed the **factors driving this quick growth**, citing a range of different factors, including AI. The incorporation of AI into personalised, consumer products has transformed smart homes for specific needs and preferences. The use of AI in consumer products generates benefits for consumers, offering convenience, informed decision-making, and encouraging continuous improvements in smart home technology, leading to more interconnected, efficient, and responsive living environments (Waite, 2024). The confidence to be able to use such devices, as well as the increasing importance placed on interoperability with other devices, also explain why the market is growing (techUK, 2023). However, there are also **barriers to the adoption** of these devices. According to the State of the Connected Home report, the biggest barrier to adoption was cost, particularly during the current cost-of-living crisis, as identified by 61% respondents to a survey of consumers. Concerns around personal privacy also featured, as did a lack of knowledge about product categories, security concerns and the belief that the technology would not meet needs or expectations (techUK, 2023).

To better understand the drivers and barriers to adoption, the use of AI consumer products should be considered in the context of AI uptake and sentiment among the wider population. A survey undertaken by the Office for National Statistics (ONS) in 2023 found that **public awareness of AI has increased**, with 72% of adults able to provide at least a partial explanation of the term AI (ONS, 2023). In terms of daily use of AI, 5% of adults said they used AI a lot, 45% a little and 50% not at all. Just over a third (34%) of adults said they had used AI chatbots in the previous month, with the most reported uses being customer service (50%), to try it out (33%), entertainment (19%) and advice (19%).

When asked about trust in AI and their expectations of the impact of AI on society, from very negative (0) to very positive (10), 32% of respondents reported a neutral impact (5). 41% of the respondents gave positive responses (6-10), while 27% gave negative responses (0-4). Of the businesses using or planning to use AI, the most common reasons provided were to improve cybersecurity and create efficiencies (both 35%) (ONS, 2023).

These data provide insights into societal attitudes towards AI and facilitate a better understanding of the current and future uses of smart and connected home products, including AI consumer products. With understanding and use of AI generally set to increase in the coming years, it can be expected that this trend will be reflected in the growing status of AI consumer products.

Market data continues to label AI and non-AI connected consumer products as smart products, with the term unlikely to change soon given its role as a buzzword in marketing and its prominence in international commodity codes. As such, it is challenging to determine the size and scale of the AI consumer product market specifically. However, data suggests that smart products are becoming increasingly popular among consumers, including those enabled with AI, such as smart speakers, washing machines and refrigerators.

Ownership levels and sales of smart products are relative and should be considered as such. According to the 2023 State of the Connected Home report, less than half of those surveyed own a smart speaker. Ownership levels of smart fitness & activity trackers, smart washing machines and smart refrigerators, while growing, remain modest if extrapolated to the wider population. Indeed, there remains potential to further increase the integration of AI in consumer products and their popularity. The figures outlined demonstrate a strong market, which is set to grow over the coming decade, following the growth trend of the wider, global AI market.

Annex 3: Reference list

AI Verify Foundation and IMDA. (2024). Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem.

Ali, S. et al. (2023). Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence.

Ambiq. (2024). A Clear Vision of Smart Glasses.

Anil, R., Dai, A. M., Firat, O., and et al. (2023). PaLM 2 Technical Report. URL https://arxiv.org/abs/2305.10403.

Argyle, L. P. et al. (2023). AI Chat Assistants can Improve Conversations about Divisive Topics.

Baba, Y. (2023). What are the harms of Smart Glasses?, *Capsule Sight*, 10 April.

Bajarin, T. (2024). The Rise Of Wearable Smart Rings, *Forbes*, 29 August.

Banabilah, S. et al. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications.

Barge, H. (2024). Being Smart with Smart Technology, *Risk Evolves*, 14 May.

Belle, V. (n.d.). Neuro-symbolic AI: Integrating deep learning and symbolic structures. The Alan Turing Institute.

Brown, T. B. et al. (2020). Language Models are Few-Shot Learners.

Boden, M. A. (2014). GOFAI, pp. 89–107. Cambridge University Press.

Boston Dynamics. (n.d.). Meta: Advanced AI Research.

Campbell, M., Hoane, A. J., & Hsu, F.-h. (2002). Deep Blue. Artif. Intell., 134(1–2):57–83, Jan 2002. ISSN 0004- 3702. URL https://doi.org/10.1016/S0004-3702(01)00129-1.

Capsule Sight. (2023). What are the harms of Smart Glasses?

Chen, S., Guevara, M., Moningi, S., Hoebers, F., Elhalawani, H., Kann, B., Bitterman, D. (2024). The effect of using a large language model to respond to patient messages, The Lancet - Digital Health, Volume 6, Issue 6, e379 - e38.

Colorado General Assembly. (2024). Senate Bill 24-205 “Concerning consumer protections in interactions with artificial intelligence systems”.

Costigan, J. (2024). China’s New Draft AI Law Prioritizes Industry Development, *Forbes*, 22 March.

Crawford, K. (2013). The Hidden Biases in Big Data, Harvard Business Review.

Cyberspace Administration of China. (2023). Interim Measures for the Management of Generative Artificial Intelligence Services.

Dotson, K. (2024). Humane unveils an AI-powered wearable smart pin that could replace your phone, *SiliconANGLE*, 9 November.

DSIT (2021). National AI Strategy.

DSIT. (2023). *A pro-innovation approach to AI regulation*.

DSIT. (2023a). Artificial Intelligence sector study 2022.

DSIT. (2023b). Frontier AI: capabilities and risks – discussion paper.

DSIT. (2024). Policy paper: Introducing the AI Safety Institute.

EU. (2024). Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act), 14 May 2024.

G7. (2023). Hiroshima Process International Guiding Principles for Organisations Developing Advanced AI Systems.

GDS and Office for Artificial Intelligence. (2020). A guide to using artificial intelligence in the public sector.

Gent, E. (2023). 'What is the AI alignment problem and how can it be solved?', *NewScientist*

Ghaffary, S. (2024). 'Pins, Monocles and Sunglasses: The Rise of AI-Focused Hardware', *Bloomberg*, 18 January.

Google DeepMind. (2023). *RoboCat: A self-improving robotic agent*.

Grand View Research. (2023). *Smart Home Market Size, Share & Trends Analysis Report By Products (Lighting Control, Security & Access Controls), By Application (New Construction, Retrofit), By Protocols (Wireless, Wired), By Region, And Segment Forecasts, 2023 – 2030*.

Gupta, A. 2024. 'What's next for generative AI: Household chores and more', *MIT Sloan School of Management*, 7 March.

Hafke, T. (2024). Generative AI in Consumer and Retail, *Alphasense*, 12 September.

Home Office. (2023). Joint Statement: Tackling child sexual abuse in the age of Artificial Intelligence.

House of Commons Science, Innovation and Technology Committee. (2024). *Governance of artificial intelligence (AI): Third Report of Session 2023–24*.

IMDA. (2022). Invitation to Pilot AI Verify: AI Governance Testing Framework & Toolkit.

insideBIGDATA. (2023). *The Rise of AI Voice Assistants: Balancing Convenience and Security*.

Intuition Robotics. (n.d.). Meet ElliQ.

Jewiss, C. (2023). 'I strapped a ChatGPT-powered monocle to my face for a week', *Stuff*, 13 October.

Johnson, E. (2024). University of York's new dressing robot mimics care workers, *BBC News*, 6 March.

Jumper, J., et al. (2021). Highly Accurate Protein Structure Prediction with AlphaFold. Nature, 596:583–589, 2021. doi: 10.1038/s41586-021-03819-2.

Kanana, B. (2024). A GPT-4V Robot That Cooks, Cleans, and Guards: EVE Android, *Cryptopolitan*, 8 January.

Kaspersky Lab. (n.d.). Smart Speaker Security - Tips to make sure your smart Speaker is secure.

Keith, M. J., Evans, C. M., Lowry, P. B., and Babb, J. S. (2014). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure, Completed Research Paper – Thirty Fifth International Conference on Information Systems.

Khalid, A. (2023). Grimes has a new line of AI plush toys, including one named Grok, *The Verge*, 14 December.

Kleinman, Z. (2024). ‘Bad at almost everything’: AI wearable panned by reviewers, *BBC News*, 16 April.

Kvartalnyi, N. 2024. ‘Exploring the Benefits of Smart Home Automation with AI’, *Inoxoft*, 24 March.

Krol, J. (2024). Oura Ring gets an AI-powered wellness advisor to help make sense of your health data, *Tech Radar*, 9 July.

Lemire, J. (2024). Smart ring maker Ōura launches generative AI-powered assistant called Oura Advisor, *Sports Business Journal*, 9 July.

Marr, B. (2024). ‘Generative AI Is Coming To Your Home Appliances’, *Forbes*, 29 March.

Marr, B. (2024a). The Biggest Consumer Technology Trends In The Next 10 Years, *Forbes*, 4 March.

Martin, A. (2023). ‘Why you may want to think twice about buying a smart appliance’, *The Standard*, 13 January.

Martineau, K. (2023). What is generative AI?, *IBM Research*, 20 April.

Mazur, B. (2024). Optimise consumer engagement with AI-enabled IoT products, *Ignitec*, 30 May.

McKinsey & Company. (2024). *What is generative AI?*.

McMahon, L. and Kleinman. Z. (2024). Glue pizza and eat rocks: Google AI search errors go viral, *BBC News*, 24 May.

Medical Device Network. (2023). AI has the potential to make smartwatches a user’s definitive health copilot.

Meta. (2024). *Designed for privacy, controlled by you*.

Meta. (2024a). *Look and ask with Meta AI on Ray-Ban Meta smart glasses*.

Meta. (2024b). Use voice controls with Ray-Ban Meta smart glasses.

MIC and METI. (2024). AI Guidelines for Business Version 1.0.

MIT Management. (no date). When AI Gets It Wrong: Addressing AI Hallucinations and Bias.

Morris et al. (2024). Position: Levels of AGI for Operationalizing Progress on the Path to AGI.

National Artificial Intelligence Research Resource (NAIRR) Task Force (2023). Strengthening and democratizing the U.S. artificial intelligence innovation ecosystem.

National Assembly of the Republic of Korea. (2023). Press Release: National Assembly Defense Subcommittee 2 passes the “Metaverse Act” and “Artificial Intelligence Act”. *Original in Korean*.

National Cyber Security Centre. (2023). ChatGPT and large language models: what’s the risk?

Newman, S. (2023). ‘Smart speakers are getting even smarter: here's what to look forward to in 2024’, *IAB UK*, 27 October.

OECD (2023). Updates to the OECD’s definition of an AI system explained.

OECD. (2024). ‘Defining AI incidents and related terms’, *OECD Artificial Intelligence Papers*, No.16, OECD Publishing, Paris

OECD. (2024a). OECD AI Incidents Monitor (AIM).

OECD. (2024b). AI creates what the 'ideal British man and woman' looks like and it will leave people divided.

OECD. (2024c). How the 'Orwellian' cameras being used by Sports Direct and Co-op work.

OECD. (2024d). 'Grinch bots' threaten to steal Christmas by driving up toy prices online.

Office for National Statistics. (2023). *Understanding AI uptake and sentiment among people and businesses in the UK: June 2023*.

OpenAI. (2021). OpenAI Codex.

OpenAI. (no date). Prompt engineering guidelines.

OpenAI. (2023). GPT-4 Technical Report. CoRR. doi: 10.48550/arXiv.2303.08774. URL https://arxiv.org/abs/2303.08774.

OPSS. (2021). Guidance: OPSS risk lexicon. 21 May 2021.

OPSS. (2021a). Study on the Impact of Artificial Intelligence on Product Safety. December 2021, prepared by the Centre for Strategy & Evaluation Services (CSES).

OPSS. (2022). Product Safety Risk Assessment Methodology (PRISM), A Guide for GB Market Surveillance Authorities and Enforcing Authorities Responsible for Regulating Consumer Product Safety. December 2022.

Orksanen, A. et al. (2023). Artificial intelligence in fine arts: A systematic review of empirical research.

Oura. (2024). Oura Ring.

Pal, K. (2023). AI Smart Glasses: Redefining Possibilities for the Visually Impaired, *Techopedia*, 14 June.

Papadopoulos, L. (2023). ‘Spider-like robotic AI arms can be attached to and controlled by humans’, *Interesting Engineering*, 7 May.

Pichai, S. & Hassabis, D. (2023). Introducing gemini: our largest and most capable ai model, December 2023.

PLOS. (2023). ‘AI experts suggest 39 percent of time currently spent on chores could be automated within the next decade’, *ScienceDaily*, 22 February.

PR Newswire. (2024). Intuition Robotics Launches ElliQ 3, Built for Scale to Meet Increasing Demand as Partnerships Expand and Adoption Grows.

Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023.

Product Security and Telecommunications Infrastructure Act 2022, c. 46.

PwC. (2018). The macroeconomic impact of artificial intelligence.

Ramesh, A., Dhariwal, P., Nichol, A., Chu, C., & Chen, M. (2022). Hierarchical Text-Conditional Image Generation with CLIP Latents. April 2022. URL https://cdn.openai.com/papers/dall-e-2.pdf.

Saharia, C., et al. (2022). Photorealistic Text-to-Image Diffusion Models with Deep Language Understanding. URL https://arxiv.org/abs/2205.11487.

Samsung. (2024). Press Release: Samsung Unveils Bespoke AI Kitchen Appliances with Technology and Connectivity That Simplify Meal Planning and Cooking, 4 March 2024.

Samuel, A. L. (1959). Some Studies in Machine Learning Using the Game of Checkers, IBM Journal of Research and Development 44:1.2 (1959): 210–229.

Sanghi Transport Company. (2023). *Smart Glasses: Revolutionizing Road Safety and Beyond*.

Sansom, A. (2024). Forget robot lawnmowers, robot gardeners are coming, *T3*, 11 March.

Silver, D., et al. (2016). Mastering the Game of Go with Deep Neural Networks and Tree Search. Nature, 529:484–489, 2016. doi: 10.1038/nature16961.

Sood, G. (2023). LG's game-changing house robot is a secret smart AI agent with numerous tricks up its sleeves, *Yanko Design*, 29 December.

Sparkes, M. (2024). AI noise-cancelling headphones let you focus on just one voice, *New Scientist*, 16 May.

St. John, A. (2022). How to Set Up a Smart Speaker for Privacy, *Consumer Reports*, 13 October.

Statista (2024a). *Smart Home - United Kingdom*.

Statista. (2024b). *Smart Home - Worldwide*.

Stockfish. (2023). Stockfish - Open Source Chess Engine.

Tech Nation. (2024). *The Tech Nation Report 2024: UK Tech in the Age of AI*.

techUK. (2023). *The State of the Connected Home 2023*.

The Business Research Company. (2024*). Smart Home Devices Global Market Report 2024*.

The White House. (2023). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

Touvron, H., et al. (2023). Llama 2: Open Foundation and Fine-Tuned Chat Models.

Tuohy, J.P. (2024). 'The much-needed reinvention of the voice assistant is almost here', *The Verge*, 14 June.

University of Maryland. (2024). Artificial Intelligence (AI) and Information Literacy.

Waite, R. (2024). *How AI Marketplaces Are Revolutionising Smart Home Technology*.

Wang, J., et al. (2022). PhenoPad: Building AI enabled note-taking interfaces for patient encounters.

Waugh, R. (2024). The robots built to take over boring household tasks, *Yahoo! News*, 16 April.

Winograd, T. (1971). Procedures as a Representation for Data in a Computer Program for Understanding Natural Language. MIT AI Technical Reports.

Contact us if you have any enquiries about this publication, including requests for alternative formats, at: OPSS.enquiries@businessandtrade.gov.uk

Office for Product Safety and Standards

Department for Business and Trade,
4th Floor Multistory, 18 The Priory Queensway, Birmingham B4 6BS
https://www.gov.uk/government/organisations/office-for-product-safety-and-standards