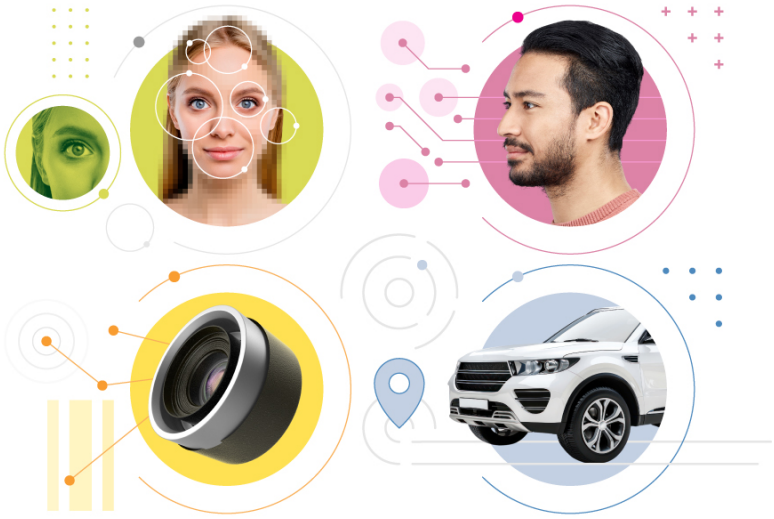
Tech Horizons report 2025

Executive summary

As the UK's data protection regulator, the Information Commissioner's Office (ICO) works to build public trust by ensuring organisations process personal data responsibly. Our aim is to empower people to share their information securely while benefiting from technological innovation.



By identifying early the privacy and data protection implications of emerging technologies, we can provide timely regulatory advice and support innovators to embed safeguards during the design phase. This third edition of Tech Horizons focuses on four technologies poised to significantly affect society, the economy and information rights in the next two – seven years:

- **Connected transport:** the convergence of technologies that is transforming how vehicles operate and interact with their environment and the people they are carrying.
- **Quantum sensing and imaging**, which offer new or radically improved capabilities compared with existing sensors and imaging technology. We focus on use cases in healthcare and medical research.
- **Digital diagnostics, therapeutics and healthcare infrastructure**, such as smart pills, digital twins and AI-assisted diagnosis.
- **Synthetic media and its identification and detection:** content that has been wholly or partially generated using AI/machine learning technologies (such as images, videos and audio) and how it is identified.

These four technologies present unique opportunities, offering potential benefits to the environment and people's health, wellbeing and mobility. However, some of the trends we

highlighted in previous Tech Horizons reports continue to apply to these technologies.

- **Emerging technologies are revealing novel types of information about people**, from brain patterns to driving fatigue. Organisations developing these technologies must build in appropriate safeguards to ensure data protection by design and by default.
- **Many new technologies collect and process increasingly large amounts of personal information**. The amount of information being collected and the complexity of its processing increase people's difficulty in understanding how organisations are using their information. This makes it important that organisations can explain what information they are collecting, how they are using it and why.
- **New technologies are being developed and used by an ever-wider range of parties, leading to lack of transparency and accountability**. As this report shows, the increasing number of innovators developing and interacting with new technologies creates complex networks. This makes it harder for people to understand who is processing their information and how they can exercise their information rights.

Many organisations continue to build data protection by design into their innovations. Others may need guidance, or to work with the regulator, to consider how they can engineer privacy into their ideas.

We will address issues proactively as these technologies mature and our role in regulating them develops. We will:

- involve the public in decisions about how we, as a regulator, address the risks and benefits these innovations may present;
- continue to invite innovators to work with our Regulatory Sandbox to engineer data protection into these technologies from the outset, focusing on the most innovative moves;
- share further insights on priority technologies by developing in-depth Tech Futures reports, such as those on neurotechnologies, quantum technologies and genomics;
- continue to work closely with our partners at the Digital Regulation Collaboration Forum (DRCF) to act on shared regulatory challenges and opportunities; and
- keep scanning the horizon for developments that require our immediate attention and possible intervention.

Introduction

Rapid advances in technology continue, bringing new regulatory challenges. As with previous Tech Horizons reports, this edition identifies some important concerns posed by selected technologies, alongside their applications and associated risks.

Our last report explored eight emerging technologies, including genomics, immersive virtual worlds, neurotechnologies and quantum computing. This third edition explores four more technologies likely to be significantly adopted in the next two to seven years:

- **Connected transport:** the convergence of technologies that is transforming how vehicles operate and interact with their environment and the people they are carrying.
- **Quantum sensing and imaging**, which offer new or radically improved capabilities compared with existing sensors and imaging techniques. We focus on use cases in healthcare and medical research.
- **Digital diagnostics, therapeutics and healthcare infrastructure**, such as smart pills, digital twins and AI-assisted diagnosis.
- **Synthetic media and its identification and detection**: content that has been wholly or partially generated using AI/machine learning technologies (such as images, videos and audio) and its detection.

In each chapter we explain the technology, explore its emerging use cases, outline its current adoption, and discuss potential future privacy and data protection risks.

- We say more about how we select and evaluate technologies in the annex.

These chapters represent our early view on often highly uncertain, evolving technology areas. You should not consider as formal guidance the data protection and privacy issues we've explored, and the recommendations we've set out in this report. They do not necessarily reflect our current or future policy positions.

For the first time, this report includes a retrospective review of selected technologies covered in previous Tech Horizons editions, updating areas of significant development. In the last year, we have also released dedicated reports on quantum technologies and genomics, which delve deeper into regulatory thinking about these emerging technologies. We have also worked with our partners in the Digital Regulation Cooperation Forum (DRCF) to publish insights on digital identity, synthetic media, and further insight into quantum technologies.

By identifying early the privacy and data protection implications of emerging technologies, we can provide timely regulatory advice and support innovators to embed safeguards during the design phase. We offer further support to organisations developing these technologies through our Regulatory Sandbox.

Connected transport

Introduction

From facial recognition of fatigue to smart watch monitoring of stress, the next generation of vehicles will know their users more intimately than ever before.

After years of growth and investment, connected vehicle technology is revolutionising the automotive industry by changing how vehicles operate and interact with people and their surroundings. Cars of the future will come equipped with advanced sensors, fast and reliable internet connectivity and sophisticated data processing abilities.

These features aim to reduce congestion, make our journeys safer and improve users' experience through seamless connection with the outside world.[1] But as our transport trends towards autonomy, the increasing use of data by vehicles raises concerns about the implications for data protection and the privacy of drivers, passengers and the wider public.[2]

State of development

The market for connected cars, cars with increased communications capabilities, has grown rapidly, with vehicle makers investing heavily to meet consumer demand for seamless, digitally enhanced in-car experiences. Advances in areas such as integrated sensors and 5G, along with new market entrants, have spurred this investment. Meanwhile, government and civil society are interested in the potential safety benefits, net-zero gains and regulatory challenges of automation.

At the heart of connected car technologies lies vehicle-to-everything (V2X) communication. V2X is a system that enables cars to communicate with:

- **other vehicles** via vehicle-to-vehicle (V2V) technology – such as allowing your vehicle to receive an instant alert warning you that a car several vehicles ahead has suddenly

braked. This feature could allow you more time to reduce your speed and avoid a collision;
- **infrastructure** via vehicle-to-infrastructure (V2I) technology – allowing your car to automatically communicate with local toll booths and pass through without stopping. This feature could reduce congestion and travel times; and
- **pedestrians** via vehicle-to-pedestrians (V2P) technology – which could enable your car to detect pedestrians carrying smart devices late at night in low visibility. The car could then take safety precautions accordingly, through enhancing headlights or reducing speed when close to the pedestrian.

V2X technology uses a combination of sensors, cameras, global positioning systems (GPS) and wireless connectivity to enable cars to collect and share this information. The technology and its data protection implications are similar to internet of things (IoT) technology and devices.[3] As with IoT, sensors collect a large volume of information in a complex ecosystem of data controllers and processors and respond in real time.

Connected car technology is regarded as nascent today. Although many new cars include advanced technology, the broader ecosystem for full connectivity is still developing. As connected technology becomes standard in vehicles and infrastructure evolves, new features and ways of making use of this capability are likely to emerge on UK roads.

Beyond V2X technology, the infotainment systems in modern vehicles are also increasingly connected. These systems are typically multimedia interfaces accessed through screens in the vehicle or an app on a user's smartphone. They include features such as:

- real-time navigation;
- voice recognition and voice assistants;
- smartphone integration;
- camera systems; and
- in-car functions.

Infotainment systems enhance driving by enabling smartphone connectivity, hands-free operation, and voice control for greater convenience and safety. Modern vehicles already feature virtual assistants for tasks like calling or texting. Emerging natural-language processing capabilities may enable vehicles to learn users' speech patterns and enhance interactions over time.[4] In-car cameras and microphones could identify occupants and customise infotainment content accordingly. In future this could include profiling and advertisements tailored to drivers or passengers based on their past verbal reactions to similar advertisements.[5]

Other features include predictive maintenance – relying on continuous data collection and analysis to provide real-time insights into vehicle health. This feature may improve vehicle performance but may also indicate a driver's routines and driving style to make efficiency

recommendations.

These technologies and use cases may first bring to mind passenger cars, but businesses in sectors such as freight and logistics have been using connected vehicle systems for many years. These include:

- telemetrics for fleet management;
- route optimisation;
- predictive maintenance on the vehicles; and
- monitoring driver hours in compliance with regulatory requirements.

These features are also used in much public transport. In future, public transport could use connected technology to enable traffic lights to automatically detect and change, creating quicker bus routes.

Smart city initiatives often look towards V2I technology to manage traffic flows in real time to reduce travel time and therefore emissions, contributing to improved health for pedestrians and residents. Similarly, these initiatives may use real-time information from connected vehicles to report on road conditions and implement safety initiatives such as reduced speed limits in icy weather.

Fictional future scenario

Sam, a marketing executive, commutes daily in her connected car. As she starts the engine, the car scans her facial features to confirm she's alert to drive. Detecting minor fatigue, the car selects an energising playlist and adjusts the internal lighting for improved focus.

The car maps the optimal route, factoring in traffic and Sam's preference for main roads. Using city-connected infrastructure, it reserves a nearby parking spot in advance for the duration of her morning meetings.

Throughout the morning, Sam's car monitors traffic patterns to suggest the optimal time to leave the office for a client meeting across town, integrating with her digital calendar and reminders app to notify her when she needs to leave. En route to a client meeting, the car's AI assistant reads her a memo from her team so she's prepared for her presentation.

On the way home from the meeting, Sam uses the infotainment system to participate in a team conference call. Using the car's external noise-cancelling features and high-speed 5G, she's able to participate in the call seamlessly. When she's 10 minutes away from home, her car alerts her home-smart devices that she'll return soon. The alert autonomously turns on her lights and speakers, and pre-heats her smart oven for dinner.

At the end of the month, a connected health and wellness app on her personal device notifies Sam that her car has noticed a pattern of increased fatigue signs on her early-morning drives. The app suggests she consider an earlier bedtime or morning workout before driving to improve her driver safety and personal wellbeing.

Data protection and privacy implications

As connected car technologies evolve, they are likely to collect and process increasing volumes of information to enable new services and features. While not all information processed will be personal, much of it may be linked to the personal information of the owner, driver or passengers. This could include real-time location data, information on driving patterns via a telemetric device or mobile app, or biometric data.

Where information does relate to an identified or identifiable person, organisations processing the information must comply with data protection legislation (UK GDPR, DPA 18).[6, 7] In addition, where data is stored and accessed on the user's terminal equipment, this will likely engage e-privacy legislation.[8]

Transparency

As connected vehicles collect a wide range of information for various purposes within a complex ecosystem of data controllers and processors, compliance with transparency requirements will remain important. The UK GDPR recognises that not all organisations involved in the processing will have the same degree of control or responsibility. Organisations must identify who is acting as a controller, a joint controller or a processor so they can clearly assign UK GDPR obligations and evidence accountability.

Organisations must provide clear, concise, and accessible privacy information. They should ensure people are clear about what information is being processed, by whom, and for what purpose. The in-vehicle environment may provide a challenge to disseminating this information, as smaller monitors and displays present less opportunity for meaningful user engagement. Organisations should also consider passengers as well as the driver.

Organisations should consider, too, when privacy notices or prompts are given because drivers must remain focused on operating the vehicle to avoid accidents. Vehicle makers should consider innovative solutions across the in-car environment – and, if applicable, mobile apps – to provide clear information when an individual is setting up the vehicle's inbuilt technologies. This should continue through ongoing real-time transparency and, where applicable, consent mechanisms throughout the vehicle's use.

Lawful basis

Once the purpose of processing has been established, organisations should take care to identify the correct lawful basis for the use of personal data within connected vehicles. They must record this in line with accountability and governance requirements. Our guide to lawful basis gives more information.

Organisations should remember that if they are storing information on – or gaining access to information stored on – terminal equipment, they must consider PECR compliance before looking at UK GDPR. In the context of connected vehicles, organisations should particularly remember Regulation 6 of PECR. This prohibits the storage and access of information on a device unless an exemption applies or consent is obtained.

If no exemption applies, prior consent must be obtained to the high standard set by UK GDPR. This requires that individuals have a meaningful way to consent without detriment, so organisations should not make consent a precondition of service. Our guidance on PECR should be consulted for more information.

Excessive data collection and online tracking

The proliferation of sensors in connected vehicles increases the risk of collecting excessive information beyond what is required for the stated purpose. In particular, sensors may collect data in a continuous and automatic way with limited or no ability for the user to effectively opt out of collection.

Under UK GDPR, organisations must collect only adequate, relevant and necessary personal information for their purposes. To adequately evidence this and meet requirements under the accountability principle of UK GPDR, organisations must clearly tell individuals what information they are collecting and for what purpose. They also must be able to show they are collecting and retaining no more than they need. As new features are installed via remote software upgrades, organisations should ensure their data collection practices are regularly reviewed to comply with these requirements.

In particular, organisations should consider if they want to collect personal information through a connected vehicle for advertising or profiling. This could include processing information from a linked smartphone or consumer-wearable device, video or audio recordings within the vehicle or use of location data from the vehicle – or a combination of these. If information is accessed or collected from these sources, PECR will probably apply.[9] In particular, organisations should remember Regulation 14 of PECR, which details strict rules on the processing of location data. Our guidance on processing location data gives more information.

If an organisation decides to process this information for advertising or profiling, they must tell individuals they want to do so and get their valid consent before starting the processing. This may be difficult in an in-vehicle environment where there are multiple

passengers or where the vehicle is shared-use. Organisations must also provide people with options to withdraw their consent at any point.

Biometric data

Connected cars of the future may rely on biometric technology to improve the vehicle's safety, security and user experience. This could range from fingerprint scanners to unlock a vehicle to internal facial recognition that authorise in-car payments at drive-thru restaurants. It may also include eye-movement tracking and facial-movement monitoring to assess the driver's health and competence at a particular point in time, enabling the vehicle to determine whether the person is safe to drive.

While these use cases have demonstrable benefits, the information collected may often be biometric special category data under the UK GDPR and therefore subject to additional protections. Even if the threshold for biometric special category data is not met, the information may still be considered sensitive and organisations should consider data minimisation and security. Our biometric data guidance should be consulted for more information.

Shared-use vehicles

Unlike many devices, vehicles are often shared, which can cause difficulty to organisations seeking to give privacy information and show compliance. A key test will be ensuring that everyone in the vehicle has access to appropriate transparency information and, where consent is being relied upon, that this is captured appropriately. This is critical so individuals understand how to enact their individual rights. Examples of shared-use circumstances could include:

- passengers in vehicles;
- rental vehicles;
- employer-provided fleet vehicles;
- company vehicles authorised for business and personal use.

Privacy concerns about shared-use vehicles centre on what information from past users can still be accessed or collected by organisations or the vehicle's future users. This could include information on the in-vehicle dashboard obtained from pairing a smartphone, or previous address locations including a marked 'home' address in a maps application.

Organisations must clearly explain what information is processed within vehicle systems and its purpose. They should also consider how to convey appropriate guidance to people about deleting information when they return the vehicle. Organisations should maintain, too, compliance with data minimisation requirements to ensure they only retain required personal information.

The nature of the sharing arrangement will determine what actions data controllers and processors need to take to comply with data protection requirements. A data protection impact assessment (DPIA) may be useful for organisations seeking to identify and minimise the data protection risks of their approach to shared-use vehicles. Our guidance on DPIAs gives more information about this.

In circumstances where information from vehicles is used to monitor employees, organisations must ensure their workers are aware of the nature, extent and reasons for monitoring. Organisations must have a clearly defined purpose for collecting and retaining the information as well as a lawful basis to rely on for this processing. Our employment practices guidance should be consulted to help employers fully comply with data protection law in this regard.

Children's information

Children are likely to be active users of vehicle infotainment systems and voice assistants. These systems include entertainment and educational materials across streaming and gaming applications delivered via an in-vehicle screen. The applications may collect personal information including account information such as a name and email address, usage data, payment information for in-game purchases or geographical information.

Organisations must therefore be aware of the UK GDPR's higher protection level for children's information. They should focus on providing default settings that ensure children have the best possible access to online services while minimising data collection and use, by default. In particular, they must be able to demonstrate a lawful basis for their processing of children's personal information, and obtain parental consent for processing under 13s' data if relying on the lawful basis of consent.

Organisations need to be aware of the specific risks and requirements relating to collecting real-time location data connected to children and restrictions regarding profiling children. Both should be switched off by default when related to children's information. If parental controls are in use in an in-vehicle environment, children should be given suitable information about this. Our Age appropriate design code provides guidance for online services likely to be accessed by children.

Recommendations and next steps

As adoption of connected car technologies grows, and as we trend towards automation, the information gathered, processed and retained by vehicles is likely to increase. These advances aim to improve safety and user experience, but this should not come at the cost of privacy. It will be critical that regulators and the broad spectrum of data controllers and processors in the vehicle industry engage to establish policies and standards about personal information that uphold consumer trust. Privacy policies should be written in a

way that's easy for people to understand and include information on how to exercise their individual rights.

Embedding privacy by design into hardware and services related to connected vehicles will be critical in supporting the various industry stakeholders such as vehicle makers, rental-car providers and public-transport operators to evidence their compliance with data protection legislation. We are committed to supporting innovators to embed privacy-enhancing mechanisms into their solutions through our array of innovation services.

Further reading

- Our updated guidance on the use of storage and access technologies
- Our 2021 consultation response to a Law Commission consultation on "A regulatory framework for automated vehicles"
- Our 2020 response to the Department for Transport's call for evidence on the Safe Use of Automated Lane Keeping System (ALKS)

---

[1] UK Gov Policy Paper on Connected and automated mobility 2025: realising the benefits of self-driving vehicles

[2] Self-driving vehicles set to be on roads by 2026 as Automated Vehicles Act becomes law - GOV.UK

[3] Our Tech Horizons report chapter on the Next generation Internet of Things provides further information about IoT

[4] The Verge article on in vehicle voice assistants getting a boost

[5] Telegraph article on infotainment system audio recordings for the purposes of advertising

[6] UK General Data Protection Regulation | ICO

[7] Data Protection Act 2018 | ICO

[8] ICO guidance on The Privacy and Electronic Communications Regulations (PECR)

[9] What are the rules on cookies and similar technologies? | ICO

Quantum sensing and imaging in healthcare

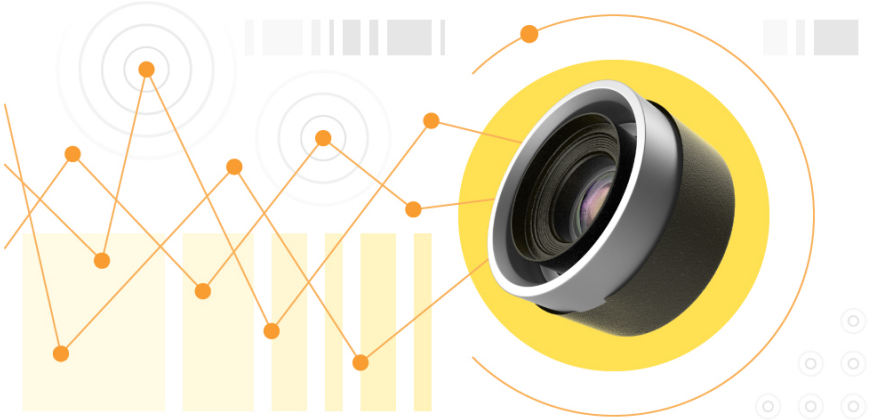
Introduction

The next generation of quantum sensors and quantum-enhanced imaging techniques offer new or radically improved capabilities compared with existing sensors and imaging techniques. They have a wide range of potential use cases in sectors such as health, defence and transport. Not all use cases will involve processing personal information.

This chapter focuses on the data protection implications of use cases in healthcare and medical research [10], which is one of the priorities for investment under the UK national quantum strategy missions. Our 2024 Tech Futures report on quantum technologies highlighted that these use cases are:

- likely to involve processing sensitive personal information;
- among the closest to commercialisation; and
- likely to expand further.

The unprecedented sensitivity of these technologies could unlock new insights into the human mind and body, and speed up the diagnosis of diseases such as cancer. In the future, combining quantum sensors with other technologies, such as medical IoT devices, could enable personalised health management at home [11].



About quantum sensing and imaging

Quantum sensors

Quantum sensors use quantum phenomena to measure subtle changes in such things as magnetic fields, gravity and temperature. These next-generation sensors give greater accuracy and precision, offering enhanced or entirely new capabilities [12]. In the future, they could also be smaller, lighter and more cost effective than current sensors for certain applications, if hardware improves and technical challenges are overcome [13].

There are many types of quantum sensor. For example, in healthcare, neuroscience and medical research, some magnetic sensors may be used for non-invasive, portable and more detailed medical diagnostics. These sensors can detect tiny changes in magnetic fields, such as changes generated by individual neurons firing in the brain or by muscle movement [14]. Potential applications include wearable brain scanners for epilepsy and Alzheimer's diagnosis and research, and cardiac health monitors detecting subtle changes in the heart's magnetic field [15].

Another type of sensor, the nanodiamond quantum sensor, can be used to speed up the diagnosis of infectious disease using a portable blood test. The sensor uses the quantum properties of a type of flaw in some tiny diamonds [16].

Quantum-enhanced imaging

Cameras using quantum-enhanced imaging use quantum effects like entanglement [17] to achieve superior resolution, contrast and novel imaging capabilities compared to existing techniques [18]. In healthcare and medical research, some of the most promising applications for quantum-enhanced imaging include improving non-invasive medical diagnostics and screening for conditions such as cancer.

One method employs ultrafast cameras with sensors detecting and timing single photons, applying machine learning to create detailed images [19]. In healthcare, this technique can be used to take pictures through some opaque surfaces, such as skin and bone (eg, to monitor blood flow in the brain), or to directly monitor tiny heartbeat variations. It could also open new possibilities for portable medical scanners in GP surgeries or ambulances (eg, to detect fractures), or could be used to improve brain-computer interfaces. Single-photon detectors could eventually support in-home monitoring for conditions like eye disease.

Another technique uses quantum entanglement to take pictures using a normal lab camera but in a wider spectrum of light than is currently possible [20]. This has applications in the biomedical imaging of cells for medical research [21].

Finally, tiny, nano-scale particles called quantum dots could enable earlier detection of cancer biomarkers, which indicate someone has the disease. These quantum dots may also be used to monitor how medicines are working in the human body. This is because they are very sensitive and interact with light in unique ways [22].

State of development

Many quantum sensing and imaging technologies are at a more advanced stage of technical development than other types of quantum technology. Plausible timescales vary according to the type of sensor. Some are already in the early stage of commercialisation,

and being used in medical research today.

The UK government is seeking to drive adoption in the healthcare sector through investment in healthcare-focused quantum research hubs [23]. The quantum missions launched in 2023 set a target for every NHS trust to have access to some quantum sensing systems for early diagnosis by 2030. Depending on factors such as evidence of clinical utility and medical device approval, we may begin to see clinical applications of quantum sensing and imaging technologies expand over the next 5-15 years [24].

Further ahead, in 15-25 years we may see the integration of certain magnetic quantum sensors in high-end consumer healthtech and wearable devices provided on prescription [25]. Quantum sensors and imaging techniques could also be integrated in future brain-computer interfaces. This could enable remote brain-health monitoring as well as commercial applications beyond healthcare, such as gaming [26].

Despite significant UK investment to date [27], there are barriers to further adoption, such as:

- commercial competition from widely used existing technologies;
- technical challenges to reduce size and cost;
- supply-chain challenges.

This means that the development and future market for many potential use cases are still highly uncertain, particularly over the next 5-15 years. We are, however, likely to see novel healthcare applications emerge as quantum-enabled research expands our understanding of the body and mind.

Fictional future scenario

Following successful clinical trials and medical device approval, several hospitals begin working with a research team to introduce wearable quantum-enabled brain scanning [28] for children with certain neurological conditions. They aim to use the system's increased sensitivity and detail as a precision tool to improve early diagnosis, treatment and monitoring of conditions such as epilepsy and autism.

Researchers conduct short brain scans in controlled clinical settings at various developmental stages. They pseudonymise the information collected and analyse it using machine-learning tools. Scan results are added to the child's medical record and stored to support future research into related conditions.

The hospital board has concerns about the increased amount of information it will need to collect and process once it starts using these systems. Before the trial, Xavier, the hospital's data protection officer, works with the research team to ensure a 'data protection by design' approach and safeguard children's information from disclosure or misuse

throughout its lifecycle.

Data protection and privacy implications

Expanded capabilities, same data protection approach

Healthcare organisations and researchers processing personal information should already be applying high data protection standards to their processing. The data protection obligations and tools to help protect this information do not change simply because future approaches may involve new quantum technologies.

The use cases we have explored in this chapter such as brain scanning, cancer screening and heart sensing will involve processing personal information. For example, they may collect data on a person's brain patterns or changes in the magnetic field of their heart, or cancer diagnostics [29]. Brain-imaging applications also involve processing neurodata, a novel and intimate type of personal information explored in our 2023 neurotech report [30].

Given the nature and context of the processing, the information collected is also likely to be health data [31], a type of special category data. Special category data needs to be treated with more care because of the potential risks to people's fundamental rights when used or the potentially severe risks of harm if unlawfully disclosed [32].

Additional protections apply to the processing of special category data. As well as identifying a lawful basis for processing, organisations processing health data must identify an Article 9 condition for processing, and ensure they maintain appropriate policy documents. The conditions relied on for this type of processing are likely to be health or social care, scientific research, or public health (Article 9, subsections (h), (j) and (i)). These conditions require additional safeguards, such as appropriate technical and organisational methods for protecting the information, and careful consideration of the purpose for processing it [33].

When testing or deploying systems that use new quantum technologies, a data protection impact assessment (DPIA) can be applied to assess the risks of processing and document any mitigations. A DPIA must be used for all processing that poses a high risk to the rights and freedoms of individuals, such as when processing special category data [34]. When completing a DPIA, organisations should consider the additional risks to people's privacy when collecting novel, more detailed insights about them.

Medical devices are regulated by the Medicines and Healthcare products Regulatory Agency (MHRA) and overseen by medical bodies such as the General Medical Council (GMC) and the National Institute for Health and Care Excellence (NICE). The interplay of the obligations these bodies impose with data protection requirements is outside the scope of this report.

Data minimisation

Organisations must only collect information that is adequate, relevant, and limited to what is needed for their lawful purpose. This is the principle of data minimisation and can help increase trust when implementing new quantum technologies.

In some health and research scenarios, organisations will not need more detail. However, in the case of novel quantum sensing and imaging for medical or research purposes, a key stated benefit over existing technologies is the extra detail and insights they provide. In the short to medium term, these technologies are most likely to be used as precision scientific tools to investigate things that current approaches cannot.

The principle of data minimisation does not prevent healthcare organisations processing more detailed information about people where necessary to support positive health outcomes. Data protection law also recognises the importance of organisations processing enough information to ensure accuracy [35]. However, organisations must have a justifiable reason for collecting and processing additional information, such as a clear clinical or research benefit. Organisations must not collect or retain more information than they need. This is part of ensuring data protection by design.

Under Article 89 of UK GDPR, organisations processing information for scientific and medical research purposes must also implement data minimisation via technical and organisational safeguards. If the research team wish to keep information beyond standard retention periods for research purposes, they must at least pseudonymise the information at the earliest possible opportunity.

UK GDPR also includes additional safeguards that the team must factor in when processing personal information for research purposes. For example, they must ensure any future research purposes are compatible with the original purpose for processing. Our guidance on the research provisions, privacy enhancing technologies, and the upcoming 2025 update to our anonymisation and pseudonymisation guidance give more information.

Enhanced capabilities may exacerbate wider risks

The new capabilities and potential for increasingly detailed insights could exacerbate existing privacy and information rights issues, should some healthcare use cases expand beyond controlled research and clinical environments. For example, while we are unlikely to see quantum technologies integrated into consumer brain-computer interfaces soon, there are already experiments exploring how quantum imaging techniques could enhance or accelerate them.

The sensitivity offered by quantum sensing techniques (such as the ability to detect individual neurons firing) and quantum-enhanced imaging, combined with potential

advances in interpreting this information, could lead to more detailed insights and inferences than people initially realise. As noted in our Tech Futures report on neurotechnology, people may not understand what information is being collected and why. If capabilities are misused or information is inadequately protected, there are concerns about risks of unfair processing (and even neurodiscrimination). The potential risks are more prominent when inferences are made about emotional responses, rather than medical conditions or diagnoses.

We are also seeing research into use cases that integrate quantum sensing and imaging techniques into in-home health-monitoring solutions. Timescales for implementation and commercialisation are unclear and we will need to remain alert to developments. As noted in our first Tech Horizons report's chapters on next-generation IoT and consumer healthtech, ensuring meaningful transparency and appropriate safeguards for special category health data will be important. This is especially so, given the additional sensitivity of new quantum techniques and the nature of the information they can be used to collect.

Recommendations and next steps

Our 2024 Tech Futures report on quantum technologies states our early thinking on the intersection of quantum technologies and data protection, including use cases for sensing and imaging beyond healthcare.

As noted in that report, to support responsible innovation and people's information rights in a quantum-enabled future, we will continue to:

- seek out further opportunities to share our insights with – and learn from – industry, UKQuantum, the UK's quantum hubs and their pilot projects, the Office for Quantum, academia, the Digital Regulation Cooperation Forum (DRCF) and other regulators; and
- explore potential applications and capabilities for quantum sensing and quantum-enhanced imaging in healthcare and any potential risks of data protection harms to people.

We also encourage further discussions with all organisations, including in healthcare and medical research, to ensure they embed privacy by design and default when testing and deploying quantum technologies that involve processing personal information.

We invite innovators to work with our Regulatory Sandbox to engineer data protection into quantum technology use cases involving personal information from the outset, focusing on the most innovative moves. We will also examine opportunities to contribute to external sandboxes and testbeds as appropriate.

Further reading

- Our tech futures report on quantum technologies

- Our guidance on lawful basis
- Our guidance on data minimisation

[10] Our recent Tech Futures report on quantum technologies explores some of the privacy implications associated with other use cases in more detail.

[11] Website for QUEST project on quantum technologies for healthcare in the home

[12] UK Quantum Sensing and Timing Hub webpage on quantum sensing: big to small technology; Regulatory Horizons Council Independent report on regulating quantum technology applications (2024)

[13] For example, interference from the external environment in real-world use cases currently reduces the accuracy of the measurements.

[14] See, eg, Website introducing a brain imaging system based on optically-pumped magnetometers (known as an OPM-MEG system); Quantum Sensing and Timing Hub webpage on sensing the brain

[15] Cureus article, The quantum-medical nexus: Understanding the impact of quantum technologies on healthcare

[16] University College London news article, Science minister announces quantum research hub for healthcare (2024); Advanced Science article on Recent Developments of Nanodiamond Quantum Sensors for Biological Applications

[17] When particles (such as two photons) are entangled, they form such a strong bond that the behaviour of one can determine the exact behaviour of the other. This effect occurs regardless of their distance apart: National Quantum Computing Centre webpage on quantum features

[18] Cureus article on The quantum-medical nexus: Understanding the impact of quantum technologies on healthcare

[19] Nature review Perspectives article on non line of sight imaging; University of Glasgow webpage for the Extreme Light group

[20] By using quantum entanglement, it is possible to measure the light that has not interacted with a cell, rather than the light that reaches the camera.

[21] Quantic webpage on seeing with undetected light.

[22] Cureus article on The quantum-medical nexus: Understanding the impact of quantum technologies on healthcare; International journal of nanomedicine article on the biomedical applications of quantum dots: Overview, challenges and clinical potential

[23] UK national quantum strategy missions

[24] Nearer-term examples include earlier epilepsy diagnosis and treatment, and using greater insights into the brain to support dementia management. Over the longer term, researchers have begun exploring how to develop handheld scanners for future diagnosis of fractures or heart conditions in GP surgeries and ambulances. For specific examples, see the ICO Tech Futures report on quantum technologies

[25] ICO Tech Futures report on quantum technologies. This includes health-tech wearables that offer more precise measures of cardiac health, muscle responsiveness and neurological health.

[26] While this use case is far off, researchers are already exploring how quantum-sensing and imaging technologies could improve future neurotechnology devices. See, eg., Webpage on using quantum imaging to accelerate research into brain computer interfaces; Innovate UK report on how UK life sciences and healthcare can benefit from quantum technologies For more about the privacy implications of neurotechnologies, see the ICO Tech Futures report on neurotechnology.

[27] Innovate UK report on how UK life sciences and healthcare can benefit from quantum technologies

[28] Known as an OPM-MEG scanner.

[29] In some cases, the information may then be anonymised.

[30] Definition of neurodata in ICO Tech Futures report on neurotechnology

[31] UK GDPR article 4(15) defines health data as personal information that relates to a person's "physical or mental health … which reveal[s] information about his or her health status."

[32] ICO guidance on special category data

[33] ICO guidance on special category data; ICO guidance: chapter on the conditions for processing special category data

[34] ICO guidance on data protection impact assessments

[35] ICO Tech Futures report on neurotechnology

Digital diagnostics, therapeutics and healthcare infrastructure

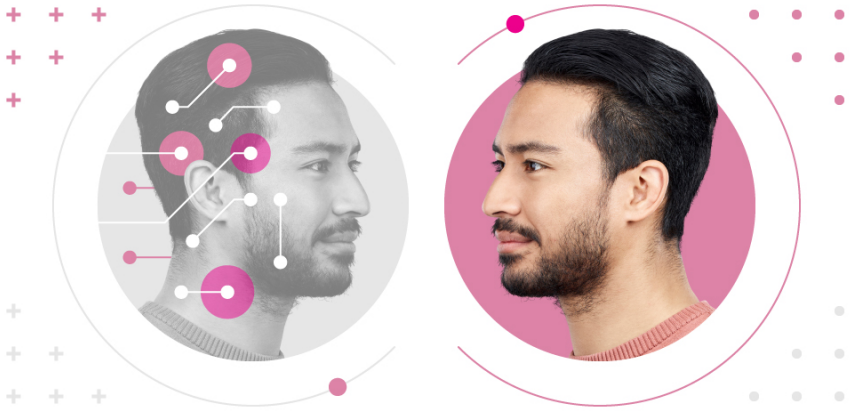
Introduction

In our first Tech Horizons report, we described how innovation was expanding the capabilities of consumer health-tech products and the potential implications for data protection and privacy. These advances in consumer health tech are mirrored by progress in regulated digital health products.

Some of these products are known collectively as digital therapeutics, which usually refers to medical interventions that are "driven by software to prevent, manage, or treat a medical disorder or disease" [36]. Alongside the rise in usage of digital therapeutics, healthcare providers have increasingly sought to digitalise other elements of health provision such as diagnosis and infrastructure.

This growth in digital health provision has been driven by several trends including resource constraints, technical advances and the impact of Covid-19. It is likely to continue as medical providers face increasing demographic pressures and are incentivised to use technology to improve efficiency [37]. The digital transformation of health is a top business priority for leaders in the healthcare industry [38] and for the Department for Health and Social Care [39]. It has also sparked regulatory interest, with the Medicines and Healthcare products Regulatory Agency (MRHA) announcing its intention for AI-powered medical devices to be available to patients "as quickly and safely as possible" [40].

In the next 3-7 years, the capabilities of digital health products could expand, further transforming medical practice. Examples include smart pills, digital twins, AI-assisted diagnosis and other digital technologies. These technologies offer significant benefits to patients, such as reduced wait times and more personalised care. The increased data they generate could augment the benefits of sharing patient data across health services [41]. However, their increased deployment and new abilities are likely to have implications for data protection and privacy.



Smart pills

Smart pills, equipped with sensors, provide medical professionals with real-time insights into patients' health (such as chemical states in the stomach) to support treatment and monitoring [42]. They can be used to monitor whether people are taking their medication, supporting those who struggle to follow their prescribed regimes [43]. The information the pills transmit is typically sent to a monitoring device or smartphone [44, 45]. Recent innovations could mean the pills become smaller and digestible [46].

Many smart-pill variations are now being developed and used to help with conditions such as HIV/AIDS, sleep apnoea and gut disorders [47]. Other uses could see the pills analyse a patient's risk of an overdose [48]. Smart pills have been trialled in the NHS [49] and related products have been used to undertake endoscopy procedures [50]. They could be used to help with remote patient monitoring alongside other innovations such as smart wards.

Digital twins

Digital twins are virtual counterparts of physical entities [51] that try to "faithfully mirror" this counterpart in real time and predict outcomes [52]. They have a wide range of applications in industry and across the wider economy, such as digital twins that replicate supply chains to help businesses respond to the risk of disruption [53].

Digital twins are already part of healthcare infrastructure [54]. In the medium term, digital twins could aid patient care by creating real-time virtual models of organs, such as the heart, and updating them with real-time data to support patient monitoring [55, 56]. Other projects have investigated the possibility of using digital twins to test patient responses to treatment, to assess therapeutic efficacy before use with patients, and to treat Alzheimer's disease and epilepsy [57]. Use as part of a patient's direct treatment could help improve outcomes by employing machine learning to achieve "a quicker diagnosis and improved treatment" [58].

Big data and advances in AI could expand the capabilities of digital twins [59], with long-term hopes of creating replicas of whole patients [60].

AI-assisted diagnosis

AI integration into medical diagnostics is expected to expand significantly over the next 3-7 years. Medical leaders hope this will help ensure patients are treated more quickly and assist in detecting a wider range of conditions [61].

The UK government has announced funding to help accelerate the implementation of AI diagnosis in areas such as stroke and lung-cancer detection [62]. Several AI-based health technologies are already supported by the NHS as part of its Accelerator initiative. Trials are in place to examine the potential for AI stethoscopes to diagnose heart failure [63].

AI diagnostic tools could personalise treatment plans for conditions like lung cancer, identifying the most effective drugs for individual patients [64]. Beyond physical health, AI diagnostic tools could accelerate the assessment and diagnosis of mental health conditions [65].

Digital infrastructure

Beyond diagnostics and therapeutics, other technologies processing personal information are increasingly deployed in healthcare to improve efficiency and patient outcomes. These include digital physiotherapists [66], virtual wards [67] and new ways of managing patients' health records [68].

One example is the use of ambient technology, which helps doctors to take medical notes when they are with patients. An app listens to the interactions between doctor and patient, then generates a set of clinical notes to be stored on the patient's healthcare record [69]. This technology has been used initially in the UK and US, and in the next 3-7 years could be widely used across the healthcare sector [70]. Its increased use could work alongside technology that automates clinicians' dictation of medical letters and other paperwork [71] and helps with translation [72].

Fictional future scenario

Niamh is in hospital after an operation. When she awakes, she can see a representation of her physiological state on a screen. This is a digital twin that represents physiological processes and is being used to monitor her recovery. The twin is continuously updated by data that comes from wearable sensors. It can be used by medical staff when assessing her condition and making decisions about her care.

As part of her recovery, Niamh is prescribed a smart pill. It contains sensors that send health metrics such as her stomach's chemical state to the doctors taking care of her recovery and to a health app on her phone. Niamh has read media articles about the privacy practices of certain health apps and hopes her data is being processed securely. The smart medication can also form part of the remote monitoring Niamh will undergo

when she goes home.

AI-enabled technologies allow medical staff to make decisions about Niamh's healthcare quickly, including her initial admission to hospital. They can recommend certain treatments and predict complications, potentially improving care. Niamh hopes she will be able to receive a full explanation of the decisions about her care and that the data used to train the systems is of sufficient quality.

Data protection and privacy implications

Cybersecurity

Healthcare data is a prime target for cyber-attacks, given the increasing digitalisation of services, the large amounts of critical digital information processed and the sometimes inadequate security measures [73].

As healthcare providers increasingly adopt digital diagnostics and therapeutics, they are likely to face growing cyber risks. Health data may be further put at risk because providers rely on legacy technology that could be vulnerable to attack from hackers even as they innovate in other areas [74]. Remote monitoring could also present a cyber security risk because of its potential for unauthorised access and data interception [75].

Healthcare providers have obligations under UK GDPR and DPA 2018, and the Network and Information Systems Regulations (NIS) may apply in some cases [76]. Obligations under UK GDPR include:

- ensuring the confidentiality, security and integrity of the personal information they process; and
- taking appropriate technical and organisational measures to protect this information.

Under the UK GDPR's data minimisation obligation, providers should only process personal data that is adequate, relevant and limited to what is necessary for the purposes of processing [77]. Compliance will also reduce the risk and impact of any cyber attacks. The use of privacy-enhancing technologies (PETs) could also help providers comply with their data protection obligations, including ensuring that relevant data gets an appropriate level of security [78].

Use of health apps

In a previous report, we identified some of the data protection issues of health products targeted at consumers, such as therapy apps [79]. Similar apps may be used to support some of the innovations described above. For example, personal data that may be generated by using a smart pill or a digital twin could be transferred to a mobile phone app to be accessed by a patient or medical professional. Such an app may be provided by a

third party.

The report identified issues with consumer-facing health apps regarding transparency and the sharing of data with app developers and other third parties. Healthcare providers that make use of apps to support some of the innovations set out above should therefore ensure they are aware of, understand and address the relevant issues affecting user privacy. These include ensuring that health apps process patients' data transparently, fairly and lawfully. Providers should also make appropriate use of internal procedures (such as the NHS's digital technology assessment criteria [80]) to ensure that app companies have in place appropriate safeguards for personal data.

AI and automated decision-making

AI and automated decision-making (ADM) [81] are increasingly used in medical decision-making [82], a trend that could accelerate in the next 3–7 years. Examples include the increased use of automated triaging and AI diagnostics that predict the efficacy of drugs [83] and analyse chest x-rays [84].

This use of AI and ADM could improve productivity and patient outcomes. However, there is a risk that using them to make decisions based on personal data, for example with triaging in high-risk contexts, could adversely affect some patients [85].

Bias and unlawful discrimination in AI systems can occur in many ways [86]. An important one is that imbalances in AI training data may statistically undervalue certain characteristics or reflect past discrimination, so an AI system could produce biased or discriminatory outcomes for patients [87]. For example, racial bias is thought to have affected the level of healthcare black patients have received in the US [88].

To prevent AI-driven discrimination, organisations should use suitable technical and organisational measures and ensure any systems used are sufficiently statistically accurate and fair [89]. The ICO has provided technical advice that can help mitigate the risk of discrimination. This could be achieved by a pre-processing technique such as adding or removing under- or over-represented population subsets. Providers will need to ensure that the processing of patients' data and use of AI do not lead to unduly harmful outcomes for patients [90].

Another risk is the potential lack of transparency in how AI tools process patient data. Transparency is a core principle of the UK GDPR, which means organisations should be clear, open and honest regarding personal information [91]. Lack of transparency in a medical setting could result in patient harm. Healthcare providers must therefore provide clear, open and concise information about how they use a patient's personal data. Using AI does not reduce a provider's responsibility to be clear about what it does with a patient's personal data and decisions based on it. This means that if an individual would usually be

given an explanation for a decision by a human, they should instead expect an explanation from those accountable for any AI-assisted decision about their healthcare [92].

There are also AI tools that use automated decision-making (ie, without any human involvement) and their increased use in the UK could at some point be feasible. Examples could include autonomous surgical robots and increasingly personalised insulin-delivery systems [93].

The UK GDPR restricts healthcare providers from making solely automated decisions that have a legal or similarly significant effect on individuals, except in certain limited circumstances. If providers fall within those circumstances, they will need to put in place extra safeguards [94]. Data about health is also considered by the UK GDPR to be special category data, which means it is more sensitive and requires extra protection [95]. If an organisation is using this data, it will need to obtain the individual's explicit consent or ensure that the processing is necessary for reasons of substantial public interest [96]. The safeguards include a requirement:

- to give individuals specific information about the processing, such as the logic used in the decision-making process;
- to take steps to avoid unlawful discrimination;
- to give individuals the right to challenge the decision.

Recommendations and next steps

As the digitalization of healthcare proceeds, we recommend that providers adopt digital solutions that implement privacy by design. To do this, they should follow our guidance on data minimisation and consider the use of PETs, where appropriate. Providers should also ensure that third party providers of health tech have in place appropriate privacy safeguards to ensure patient data is processed transparently. Additionally, as AI is increasingly integrated into health provision, providers will also need to follow guidance about fairness, bias and unlawful discrimination. Ensuring that personal information is processed fairly, transparently and lawfully will allow patients to reap the full benefits of the changing healthcare industry.

Innovators can receive support in embedding privacy by design through our range of innovation services. As the digital healthcare landscape continues to develop rapidly, we will monitor new use cases as part of our wider work.

Further reading

- Our guidance on fairness, bias and discrimination in AI
- Our guidance on automated decision making
- Our guidance on lawfulness, fairness and transparency
- Our guidance on data minimisation

[36] European Data Protection Supervisor report on Digital Therapeutics

[37] House of Commons Library article on capacity pressures in health and social care in England

[38] Deloitte article about 2025 health care outlook

[39] Health and Social Care Committee report on Digital transformation in the NHS

[40] MHRA trials five innovative AI technologies as part of pilot scheme to change regulatory approach - GOV.UK

[41] UK Government article on using NHS data to improve healthcare

[42] CNN article on smart pills and their risks

[43] Ibid.

[44] MIT News article on smart pill tracking key biological markers in real-time

[45] Soracom article about smart pills sharing patient data

[46] Ibid

[47] Medscape article on how smart pills will transform personalized care

[48] Ibid

[49] NHS 2018 trial of smart pills

[50] NHS use of capsule cameras to test for cancer

[51] University of Nottingham article about 'Digital twin' heart modelling project

[52] NPJ digital article on Digital Twins for health

[53] McKinsey article on digital-twin technology

[54] Glasgow City of Science & Innovation article on use of digital twins

[55] Imperial College London article on 'Digital twin' heart modelling project

[56] The Guardian article on how digital twins enables personalised health treatment

[57] U.S. GAO article on Virtual Models of People and Objects

[58] U.S. GAO article on Virtual Models of People and Objects

[59] NPJ digital article on Digital Twins for Health

[60] Ibid

[61] Axios article on AI disease diagnosis

[62] Gov UK- AI to speed up lung cancer diagnosis deployed in NHS hospitals

[63] Imperial College London article on AI stethoscope being rolled out to 100 GP clinics to help diagnose heart failure

[64] National Institute for Health and Care research article on AI in healthcare

[65] Universitat Oberta de Catalunya article on artificial intelligence and the future of healthcare

[66] The Guardian article on the First NHS physiotherapy clinic run by AI

[67] NHS England - Virtual wards

[68] NHS England - NHS Federated Data Platform (FDP)

[69] Digital Health article on automated AI-powered clinical documentation

[70] Daily Mail article on automated notetaking for GPs

[71] NHS Transformation Directorate - Using an AI-driven dictation platform to free up clinicians' time

[72] Stanford Medical article on the promise and pitfalls of AI in medicine

[73] Action Santé Mondiale article about application of AI to healthcare [also: Cyber-attacks on critical health infrastructure]

[74] Article in HT World about legacy tech

[75] Journal of mHealth article about the cyber security risks of remote monitoring

[76] The Network and Information Systems Regulations 2018: guide for the health sector in England - GOV.UK

[77] Principle (c): Data minimisation | ICO

[78] How can PETs help with data protection compliance? | ICO

[79] ICO Tech Horizons Report 2022

[80] Digital Technology Assessment Criteria (DTAC) - NHS England

[81] What is automated individual decision-making and profiling? | ICO

[82] Medical Law Review about Automated Decision Making

[83] National Institute for Health and Care about how artificial intelligence is making it easier to diagnose disease

[84] NICE article on the use of AI to analyse chest x-rays

[85] What about fairness, bias and discrimination? | ICO

[86] Ibid.

[87] Ibid.

[88] Article in Science about dissecting algorithms to manage the health of populations

[89] What about fairness, bias and discrimination? | ICO

[90] How do we ensure fairness in AI? | ICO

[91] Principle (a): Lawfulness, fairness and transparency | ICO

[92] Definitions | ICODefinitions | ICO

[93] Medical Law Review about Automated Decision Making

[94] Rights related to automated decision-making including profiling | ICO

[95] What is special category data? | ICO

[96] Rights related to automated decision-making including profiling | ICO

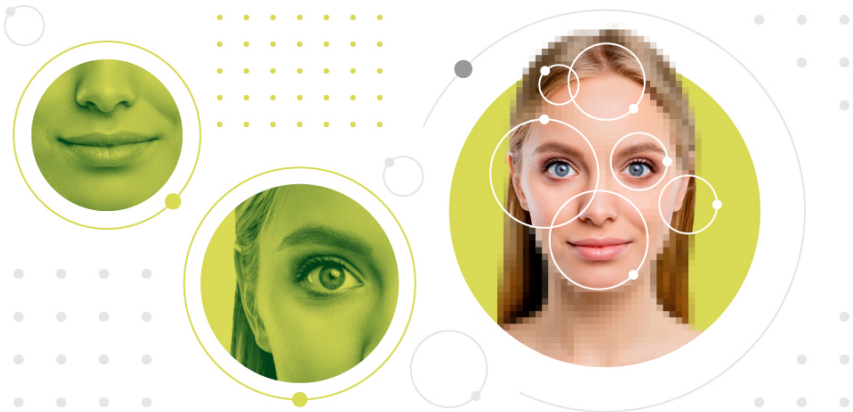
Synthetic media and its identification and detection

Introduction

Synthetic media refers to content partially or entirely generated using AI or machine learning, including images, video and audio. It is already used in entertainment, advertising, and personalised content.

Personal data is often used in the creation, distribution and targeting of synthetic media. This can include the use of biometric information used to train the AI models to generate realistic-looking people, or to insert or substitute individuals into media.

As synthetic media technology has advanced, distinguishing deepfake content from real media has become increasingly difficult, creating a pressing need for reliable identification and detection methods. This chapter looks at what technological and social means could be used in future as the quality of synthetic media improves, to protect individuals and their data.



Protecting against malicious synthetic media and deepfakes

Deepfakes are among the most controversial applications of synthetic media. The Oxford English Dictionary defines a deepfake as "[a]ny of various media, [especially] a video, that has been digitally manipulated to replace one person's likeness convincingly with that of another, often used maliciously to show someone doing something that he or she did not do."

Malicious uses of synthetic media are designed to be convincing, so that a viewer might be fooled into believing that the events that they depict really happened. As the technology used to create synthetic media has advanced, synthetic media and deepfake content has become less obviously fake. This has created a need for methods to separate artificial

content from real.

Both the public and private sectors have seen initiatives to address this need, including the Home Office's deepfake detection challenge (and in the US) the Tech Accord to Combat Deceptive Use of AI in 2024 Elections, which specifically addressed the use of deepfakes to create election disinformation.

The EU AI Act [97] requires providers of AI systems generating synthetic content to ensure outputs are marked as artificial in a detectable, machine-readable format. This places responsibility on creators to prevent misuse.

State of development

As the volume and sophistication of synthetic media and deepfakes is likely to increase in future, so must the measures used to detect them and malicious uses of them.
Various methods might be used to allow individuals and organisations to determine if a piece of media is original and unaltered or has been generated or manipulated by AI.

Responsibility for transparency may be placed on the:

- creator of the media;
- organisations providing the tools to create the media;
- organisations acting as intermediaries in the storage or sharing of that media. Creators of malicious synthetic media are unlikely to comply with schemes marking content as manipulated, placing greater responsibility on hosting platforms to flag or remove such content. In the future, the absence of verification may increasingly signal that content has been manipulated.

The following measures are being developed or in some cases are already on the market. To be effective, they will need to keep pace with the sophistication of synthetic media.

Certification of the provenance of media

Certification of provenance focuses on allowing creators or custodians of a piece of content to store information about it. This might include how the media was created and by whom. Another use might be showing whether it is original and unaltered or is artificially generated or manipulated.

Several large technology companies, as well as media and synthetic content creation organisations, are members of the Coalition for Content Provenance and Authenticity [98]. This initiative provides a technical standard [99] that creators and publishers can use to certify their media, allowing individuals to establish whether what they've received has been altered.

Watermarking

Related to the idea of certification of provenance is the idea of 'watermarking' content. Adding a watermark to content to show it is synthetic works in a similar way to watermarking a still image. A signifier is inserted into the media, which can then be read to show its origin. In the US in 2023, the president signed an executive order requiring watermarking tools to be developed for government communications to protect citizens from disinformation.

Current watermarking tools are reportedly vulnerable to tampering [100] and may degrade media quality [101], raising questions about their long-term efficacy [102].

Systematic detection of synthetic media

AI – the technology that makes synthetic media and deepfakes possible – can also be used to analyse media and determine whether it has been generated or manipulated artificially.

Systematic or automated detection systems rely on inconsistencies or characteristic signs of editing in (for example) facial expressions or vocal patterns that might not be immediately apparent. This might mean looking for a mismatch in the shape of a mouth (the 'viseme') and the sound coming out of it (the 'phoneme') or picking out the boundary where the original material and the inserted material have been blended. Often, tests are run on the same piece of media to create an aggregated risk score.

If an automated system used to detect synthetic media itself processes personal information as part of the analysis, it will need to comply with data protection law.

Account reputation and behaviour-based measures

Account reputation-based filtering and moderation has been used in other platforms and for other media to try to limit spam and offensive content. These measures look not just at the content, but who is creating and sharing it. If those individuals or accounts are rated poorly for conduct or accuracy, content shared from them can be filtered out or otherwise limited.

This sort of detection and intervention could be performed by 'human fact-checkers', for example, or platforms could use automated means to detect behaviours that looked suspicious.

Social measures and media literacy

As synthetic media becomes a larger portion of what is created and shared by individuals, we will need to understand the changing nature of our relationship with shared media. This may mean a fundamental shift in whether we trust received media by default or not.

Education about how people can protect themselves from harms caused by malicious uses of synthetic media and deepfakes may complement the technical measures described in

this chapter. An analogy is how people have been educated to recognise spam email. In future we may see media that is suspect treated in the same way as today we regard spam email promising riches.

Regardless of the methods employed, the role of human identifiers, moderators and fact-checkers will probably expand with the need for an 'expert eye' to supplement detection systems. Humans would act to offer a second line of identification for anything that met a criterion of likely synthetic origin that was detected by automated means.

Fictional future scenario

Simran, a finance officer for a large construction company, receives an email from their company's finance director, with an invoice attached. The invoice is for a large sum for an organisation Simran doesn't recognise.

The email seems genuine, but the company has previously given employees training about recognising cyber threats, so Simran decides to email the director to query the invoice. They receive an out-of-office reply from the finance director. However, the email with the invoice attached has a number to call about any issues. Simran calls it and the person at the other end sounds like the finance director. The director seems to be in a hurry to complete the call, though, and urges Simran to make the payment.

Now suspicious, Simran asks for a video call to make sure everything is above board, and the finance director reluctantly agrees. When the video call comes in, again it appears to be the director speaking, and their voice seems normal. However, Simran's company has invested in technology for its videoconferencing suite that detects synthetic media, and it alerts them to the high probability that both the video and voice have been manipulated.

Satisfied, Simran terminates the call, reports the email as a 'spear phishing' scam, and emails their IT department to alert them to the scam.

Data protection and privacy implications

Where personal information is used in developing or using models to create synthetic media, data protection law applies. This is true even if the final synthetic media doesn't contain any personal information.

Personal information is also likely to be used in the identification and detection of synthetic media. Here, we focus on the data protection and privacy implications of such methods.

Certification of provenance and watermarking

Personal information may be processed in a provenance certification system or watermarking system – for example, if the identity of the creator of a piece of media is

recorded, or their location data.

Under these circumstances, organisations controlling or processing that personal data will need to be aware of their responsibilities under data protection law, including how to address rights requests made by individuals. These might include rectification of inaccurate data stored within the certification process or watermark, or erasure of personal data that has been recorded – which might affect the validity of the certification or watermark.

Systematic detection of synthetic media

Measures designed to identify and classify media as either original or manipulated by AI may be processing personal information as part of that identification process.

Analysis of multimodal media in comparison to samples of known 'real' examples from individuals would be likely to be processing the personal data of those individuals during the comparison. For example, if a piece of video (which may have been altered) of a world leader is analysed, that information relates to an identifiable person, so the analysis is likely to be processing personal information.

Automated content moderation

If automated moderation is used (regardless of the detection method), platforms must comply with Article 22 of the UK GDPR. This grants individuals rights regarding decisions made solely through automated processing where it has a legal, or similarly significantly life-affecting impact. The ICO has previously produced guidance for organisations considering using automated decision making for content moderation.

Security

Deepfakes and synthetic media can be used to fool recipients into taking actions they would not normally take. Here, malicious synthetic media and deepfakes might be used to:

- bypass authentication systems by using a deepfaked identity;
- persuade people to divulge personal information for criminal or malicious purposes including blackmail once trust has been gained;
- convince people to make payments to scammers, such as authorised push payment fraud [103];
- disinform for political or ideological ends.

These outcomes might have additional data protection implications, including upholding the security of data stored. Organisations must use appropriate technical and organisational measures to secure the personal information they process [104]. This would include protecting it from unauthorised access or damage by those using deepfaked identities.

Recommendations and next steps

As technology advances and capabilities improve, so too will the quality and ease of creation of synthetic media. While this may lead to a greater adoption in the arts and culture, entertainment, and education, malicious uses of synthetic media are also likely to remain present or increase. This will make the ability to identify and detect where media has been manipulated increasingly necessary if people are to be protected. Therefore, those who build or maintain systems that identify or detect synthetic media will need to ensure they do so in a manner compliant with data protection law (if those systems are processing personal data). Building in data protection by design to systems designed to watermark, certify or analyse content or its distribution will ensure that users are confident their personal data is being handled appropriately.

To better help controllers who are or will be using synthetic media identification and detection, the ICO will:

- develop our understanding of the processing of personal data within synthetic media and its detection/identification, including as a subset of our work on generative AI;
- work with other regulators (including through the DRCF) to build our knowledge of the effects of synthetic media and its detection, and identify areas of critical regulatory intersection; and
- continue to engage with the public, academia, interest groups and industry about synthetic media and its identification and detection.

The ICO is committed to enabling responsible innovation and supporting organisations that are thinking of developing synthetic media identification and detection systems. Our innovation services aim to help innovators bring privacy-respecting products and services to market.

Further reading

- Our guidance on how to process biometric data lawfully
- Our response to the consultation series on generative AI
- Our guidance for organisations considering the use of automated decision making in content moderation
- Our guidance on automated decision-making and profiling

---

[97] Art. 50 Transparency Obligations for Providers and Deployers of Certain AI Systems - EU AI Act

[98] The home page of the Coalition for Content Provenance and Authenticity

[99] C2PA specification implementation guidance

[100] An MIT technology review on removing watermarks from text

[101] A paper by K. Singh and J. Zou on quality degradation due to watermarking

[102] A paper on the robustness of AI-image detectors by Saberi, M., Sadasivan, V. S., Rezaei, K., Kumar, A., Chegini, A., Wang, W., & Feizi, S.

[103] The Payment Systems Regulator's page on authorised push payment scams

[104] The ICO's guide to the data protection principles

Updates on previous technologies

Introduction

Each Tech Horizons report features regulatory snapshots of technologies projected to significantly affect personal data. We select technologies through structured horizon-scanning and prioritisation. Our reports represent the start of our work to understand emerging technologies, not its conclusion.

Here, we present updates on our continued work to prepare for the effect of emerging technologies featured in our previous Tech Horizons reports.

Consumer health tech

Consumer health tech continues to develop, as do its implications. Smart watches can now collect more health-related data such as sleep apnoea detection [105]. Other consumer tech has received US Food and Drug Administration approval for use as hearing aids [106] . Research continues into the capabilities of smart fabrics to monitor health metrics.

We continue to scrutinise this market. An ICO-commissioned poll of women's health app users revealed widespread concern about developers' approaches to privacy, including transparency and data security practices [107]. This concern led to our recent review of a range of these apps. We set out several practical recommendations for developers including the need to:

- be transparent and accountable;
- obtain valid consent where appropriate; and
- establish an appropriate lawful basis [108].

These recommendations also apply to health app developers more generally.

Commercial use of drones

The use of drones continues grow rapidly in the UK. The UK Civil Aviation Authority (CAA) published its roadmap for the development of drones for use on beyond visual line of sight (BVLOS) in Autumn 2024, setting a target of establishing routine BVLOS operations in the UK by 2027.

Several trials are underway to support this, exploring use cases noted in the second edition of Tech Horizons report including deliveries to consumers by drone, medical deliveries and remote infrastructure inspection.

We continue to work on the commercial use of drones through our Regulatory Sandbox. Kestrix entered our Regulatory Sandbox in 2024, seeking to explore the use of drones to capture mass thermal images to enable energy retrofits of existing buildings at scale. We will publish a report on our data protection conclusions at the end of our engagement with Kestrix later this year.

Personalised AI

AI and its applications in industry and the home has been a topic of widespread interest. We continue to develop our position on responsible use of information in these innovative systems. As the technology matures, personalised AI on-device could empower users, without controllers needing large-scale data collection and processing.

In early 2024, at the time of the publication of the Tech Horizons report on personalised AI, we launched a series of calls for views as part of a consultation on how data protection law should apply to the development and use of generative AI models. Generative AI is developed and deployed in ways that are distinct from simpler AI models used in classification or prediction.

Our response to the consultation series on generative AI summarises some of the key themes from the consultation responses. It also sets out our thinking on how areas of data protection law apply to generative AI systems and makes a commitment to update existing guidance in line with the consultation findings and response.

Next-generation IoT

The IoT industry is becoming increasingly sophisticated and integrated with AI, including in examples of novel smart-home devices. This includes embedding new versions of generative AI and large-language models in powerful smart-home devices to improve the understanding of complex verbal and written queries [109].

We held a roundtable with IoT manufacturers to understand the challenges manufacturers face and conducted a citizen's jury [110] to understand the public's perceptions and expectations of IoT. The research explored six areas of data protection: consent, transparency, profiling and advertising, individual rights, accountability and security.

The results of the citizen's jury will inform our drafting of guidance on consumer IoT, which we will publish this spring. The guidance will help to provide certainty and clarity to industry and developers, encouraging them to build in privacy by design and default.

Since publishing the Tech Horizons report chapter on next-generation IoT, we've accepted an IoT project into our Sandbox from Eclipse Digital Solutions and Geutebruck (UK) to explore the privacy aspects of their novel IoT system. This system uses a combination of sensors and AI to predict and prevent falls in such settings as hospitals and adult social care [111].

Quantum technologies

Quantum computing and communications technologies continue to advance, with research making wider long-term deployment more viable. Developments in hardware, software and error mitigation are helping pave the way to a more advanced, scalable quantum computer. In quantum communications, researchers from the UK have used existing subsea network infrastructure to show that quantum key distribution is possible over longer distances.

The ICO's tech futures report on quantum technologies explores the issues raised in the previous Tech Horizons report chapter on quantum computing in far more detail, and explores the transition to post-quantum cryptography. The report covers the range of quantum technologies, from quantum sensing, timing and imaging to quantum computing and quantum communications. It considers use cases such as medicine, finance, communications and law enforcement and explores how long they may take to develop.

In December we published an update to our previous work on Quantum technologies with the DRCF. This reflection on developments in the quantum ecosystem covers advances in the technologies, as well as providing insight into evolving thinking on regulation and standards.

Neurotechnologies

International interest in neurodata and its privacy implications has continued to increase in the past year. Forthcoming reports include UNESCO's Recommendation on the Ethics of Neurotechnology and papers from the Global Privacy Assembly and the International Working Group on Data Protection in Technology (IWGDPT).

Neurotechnologies have continued to develop, with uses such as home treatment for mental health purposes being discussed as devices become cheaper and more available. In the US, two new laws regulating 'neural data' have been passed in Colorado and California, each clarifying that neural data is 'sensitive data' under both states' underlying consumer privacy laws. This is a different approach to that of other countries where the creation of new 'neurorights' expands existing privacy laws instead.

In 2023 we published our tech futures report on neurotechnologies, a rapidly developing sector that uses information directly taken from the brain. This information can be used to predict, diagnose and treat complex physical and mental illnesses. It will probably lead to applications in the workplace, education, sport and entertainment.

We will address areas of concern by producing neurotechnology-specific guidance. The guidance will meet the need for regulatory clarity and set clear expectations about the definition and use of neurodata in a responsible manner, compliant with data protection law.

Immersive futures and technologies

The immersive technology industry continues to expand as new devices are launched and further use cases established. Advances in augmented reality capabilities include increased smart-phone integration, allowing for a wider user-base than standalone head-mounted devices. Consumer use cases include gaming, entertainment and immersive shopping experiences. Elsewhere in industry, organisations are using extended reality (XR) technology for virtual training and collaboration across a broad range of sectors including manufacturing and health.

Our work on immersive technologies spanned the first and second editions of our Tech Horizons reports, initially reviewing privacy concerns related to extended reality hardware and expanding into the more nuanced visions of future virtual worlds.

We have progressed this work in collaboration with other digital regulators within the DRCF, culminating in an Immersive Technologies Foresight Paper. The paper considers how immersive environments might evolve and the key uncertainties that could drive changes to them. It also sets out the potential regulatory implications that may arise across privacy, competition, financial and communication policy in the UK.

We have also continued our work on immersive technologies through accepting an augmented reality (AR) based application into our Regulatory Sandbox. CrossSense, developed by Animorph Co-operative, is designed to empower people living with dementia to maintain their independence, using smart glasses and AR technology.

Genomics

As genomic analysis continues to mature technologically and as an industry, we are seeing initiatives aimed at helping people understand the fundamental scientific principles behind it.

These initiatives focus on resolving concerns by enabling conversations about genomics more widely. Part of addressing distrust and fear around genomic technologies is normalising the discussion of them, which projects like Only Human (of which Genomics England is a founding partner) seek to do.

Set against a background of increasing interest and investment in applications including health insurance and education, the ICO Tech Futures: emerging genomics report expands on the thinking in our previous Genomics Tech Horizons report chapter. The report includes insight on when genomic data may be considered personal information and the challenges around the use of intrinsic third-party information. It also highlights the significant risks of bias and discrimination that can emerge from processing genomic information.

The report outlines our commitment to engage with the public to better understand their concerns about the use of genomics and privacy. Facilitating engagement and increasing knowledge about genomics will help to strengthen people's abilities to play an informed role in the technology as it develops. By continuing to engage with key stakeholders across industry, regulation, academia and civil society, we will ensure that building data protection into uses of genomic information is fundamental to their development. This will include inviting organisations to work with our Regulatory Sandbox.

---

[105] A ZDNET article on the Samsung Galaxy Watch's FDA clearance

[106] An NPR article about the FDA approving some Apple AirPods as hearing aids

[107] ICO to review period and fertility tracking apps as poll shows more than half of women are concerned over data security | ICO

[108] ICO urges all app developers to prioritise privacy

[109] A CNET article on Google integrating AI into search

[110] The ICO's report on the results of its IoT citizen's jury

[111] Current projects within the ICO's sandbox

Annex: Our methodology

The selection and evaluation process behind the four technologies we've explored in this report was guided by a robust, horizon-scanning and foresight process. This consisted of four consecutive phases that have been refined through our previous two reports:

Phase 1: Horizon scanning

This initial horizon-scanning phase focused mainly on identifying a longlist of emerging technologies for us to consider for inclusion in the report. This process relied on a so-called 'scan-of-scans' approach, in which we collated and contrasted technologies and emerging trends explored in recent foresight and technology publications. Our scan considered numerous high-quality sources from a wide range of countries and stakeholder communities to ensure a diversity of perspectives. This identified more than 50 possible technologies.

Phase 2: Prioritisation

In the second phase, we narrowed this longlist of technologies to the final four priority topics. This shortlisting involved rigorous evaluation and stress testing in which we scored potential technologies on several qualitative and quantitative indicators.

These indicators aimed to show:

- the magnitude and novelty of the possible privacy risks associated with an emerging technology (with an emphasis on harms disproportionately affecting those groups most at risk of harm, and the potential processing of special category information);
- the expected maturity and market penetration of an emerging technology over the next two to seven years;
- the degree and pace of innovation driving an emerging technology's development (with a preference for technologies that have undergone significant change over the past 18 months across a range of sectors).

Phase 3: Evaluation

During the third phase, we explored each of the four priority topics in more depth, and stress-tested conclusions about possible future privacy and data protection considerations with external experts.

Phase 4: Scenario-building

The fourth and final phase explored the possible trajectories our priority technologies may follow in the years ahead. We developed scenarios that aimed to shed further light on the privacy and data protection implications of these different possible futures. We carried out scenario-building exercises not just to map the most direct emerging effects and use cases of a technology, but also the more speculative second-order effects they may generate ("don't predict the car, but the traffic jam"). Each of the subject-specific chapters includes an example box describing what people's day-to-day interactions with a new technology might look like in the future.

Annex: Glossary

Connected Car / Connected car technology	Systems that equip cars with increased communication technologies, allowing for communication between vehicles (vehicle-to-vehicle or V2V), between vehicles and infrastructure (V2I) and between vehicles and pedestrians (V2P). Collectively Vehicle-to-everything (V2X) technology uses a combination of sensors, cameras, global positioning systems (GPS) and wireless connectivity to enable cars to collect and share information.
Digital twins	Digital twins are virtual counterparts of physical entities that try to "faithfully mirror" this counterpart in real time and predict outcomes. They have a wide range of applications in industry and across the wider economy, such as digital twins that replicate supply chains to help businesses respond to the risk of disruption.
Entanglement	One of the quantum phenomena used to unlock new capabilities. When particles (such as two photons or electrons) are entangled, they form such a strong bond that the behaviour of one can determine the exact behaviour of the other. This effect occurs regardless of how far away they are from each other [112]. Quantum technologies use this property to help securely share information, or to take ultra-precise measurements and images at the atomic level, even at a distance, in low light, or outside the line of sight.
Generative AI	Artificial intelligence models that can create new content eg text, computer code, audio, music, images, and videos. Typically these models are trained on extensive datasets, which allows them to exhibit a broad range of general-purpose capabilities.
Genomics	A relatively recent branch of scientific study focused on the study of the entirety of a person's DNA sequence (the genome). It looks at the interplay of genes with each other and their environments and how these can impact our traits and characteristics.

Internet of Things (IoT)	The network of physical objects ('things') that can connect and share information with other things and systems over the internet. These 'things' can sense, respond to or interact with the external environment. IoT includes both consumer devices eg smart TVs or smart speakers, and industrial systems.
MRHA	Medicines and Healthcare products Regulatory Agency. Responsible for regulating medicines, medical devices and blood components for transfusion, in the UK.
Nanodiamond Quantum sensor	An emerging sensor technology that uses the properties of a lattice of carbon atoms with specific chemical impurities to potentially allow for new types of sensor applications, including in biology and medicine.
Nano-scale	Measurement scales used for extremely small objects, such as DNA. A nanometer is one-billionth of a meter. As an example, a human hair is approximately 80,000-100,000 nanometers wide.
Neurotechnologies	A group of technologies and procedures that allow for the monitoring, assessing, emulating and manipulation of functions of neural systems, including the human brain. Examples include brain to computer interfaces, prosthetics and diagnostic devices.
Neurodiscrimination	A new type of discrimination we may see in future resulting from, among other things, inaccurate or biased analysis of neurodata. For further information see the discussion in our Tech futures report on neurotechnologies.
Sandbox	Sandboxes are programmes that allow new products or services to tested in a controlled environment. the ICO Regulatory Sandbox is a free service developed by the ICO, to support organisations who are creating products and services which utilise personal data in innovative and safe ways. Participants have the opportunity to engage with our Sandbox team, to draw upon our wider ICO expertise and advice on mitigating risks and embedding 'data protection design'.
Smart cities, or smart city initiatives	An aspirational term with a contested definition encompassing attempts to increase the integration of physical, digital and human systems in the built environment. Typically pursued

	with the ambition of creating cities that are sustainable, liveable, resilient, and able to make more efficient use of limited resources.
Smart pills	Small ingestible technologies equipped with various sensors and capable of transmitting information to external devices. Also known as digital pills.
Use cases	The anticipated, imagined or expected uses for a technology in development. Uses cases typically inform the design or a technology as it becomes adapted into products and services.

[112] NQCC webpage on Quantum features