Innovation and Technology

ICO tech futures: Quantum technologies

ico.

Information Commissioner's Office

Executive summary

Quantum technologies harness the principles of quantum mechanics to offer revolutionary advances in computing, communications, sensing, timing and imaging. They encompass a broad range of enabling technologies, with potential applications across diverse fields from medicine to finance, defence, law enforcement, materials science and public infrastructure.

As the UK's data protection regulator, we want to ensure that people's personal information [1], privacy and information rights are protected in a quantum-enabled future. We also want to encourage the UK's quantum industry to innovate responsibly, and consider any privacy implications at an early stage. This report examines what a quantum-enabled future could look like, through a data protection and information rights lens.

This report spans the range of quantum technologies, from quantum sensing, timing and imaging to quantum computing and quantum communications. It considers use cases in domains such as medicine, finance, communications and law enforcement and explores when they may develop. While many applications that are relevant to us will not emerge until the medium to long term, some impacts are being felt now.

In particular, we are seeing the first steps towards the future "state of the art" in cyber security in response to the expected impact of quantum computing on cryptography. Larger organisations, such as digital service providers or financial service providers, should start to prepare for the transition to post-quantum cryptography [2]. This could include identifying and reviewing their at-risk information and systems, while also maintaining good resilience against existing cyber risks. People and smaller organisations using standard operating systems should keep up-to-date with regular software updates. This will help to protect their devices and systems against current and future cyber risks.

Beyond information security issues, the advanced capabilities and convergence of quantum and classical technologies may exacerbate some existing privacy risks in future. As well as enable new opportunities to protect personal information. Material risks to people's privacy are more likely to arise if applications of these technologies are misused or not deployed lawfully, fairly and transparently, or without regard to people's rights and freedoms.

At this early stage, industry and the ICO have a promising window of opportunity to engage and learn from each other. To help work towards a quantum-enabled future, we will:

- continue to work with the National Cyber Security Centre to raise awareness of cyber security risks arising from quantum computing, updating our guidance on encryption in line with the transition to post-quantum cryptography;
- continue to engage with, learn from and share our perspective with industry, the National Quantum Computing Centre, the UK's Quantum Hubs, the Office for Quantum and other regulators on developments in wider quantum technologies; and
- consider sandbox applications for any quantum technology use cases likely to come to market in the next three years that may involve processing personal information.

This report represents our early-stage thinking on the intersection of quantum technologies and data protection. We do not intend it as guidance. Should you wish to continue the conversation, please contact us at: [email protected].

[1] any information relating to an identifiable living individual.

[2] Post-quantum cryptography: what comes next? - NCSC.GOV.UK; Next steps in preparing for post-quantum cryptography - NCSC.GOV.UK. The NCSC defines a large organisation as one with more than 250 employees.

Introduction

Quantum technologies are enabling technologies that work in a different way to their classical counterparts. They make use of quantum phenomena to unlock new capabilities and could be used in many different future applications. Many of these technologies are still at an early stage of development, such as quantum computers. Others are already commercialised, such as certain next generation quantum sensing technologies. Researchers and business are still exploring potential real world use cases. For example:

- **Quantum computers** have the potential to solve certain problems exponentially faster than the computers we use today. This includes some problems that current computers effectively cannot solve. Potential applications cover a range of industries including physics, finance, materials science and medicine.
- The next generation of **quantum sensors** and advanced **quantum timing** technologies (optical clocks) have the potential to reach unprecedented measurement precision. Potential applications include medical diagnostics, urban infrastructure and environmental resource management, climate change planning, surveillance and jamming-resistant navigation for defence.
- **Quantum enhanced imaging** techniques could enable new functions, such as cameras that:
  - detect the presence of people and objects around corners or through walls;
  - more accurately identify molecules inside the body; or
  - provide clear images, even in foggy or congested environments.

The different techniques have potential applications in fields like medical research, autonomous vehicle safety, defence and law enforcement.

- **Quantum communications** offer a new method for securely sharing cryptographic keys. They use the physical properties of light in a quantum state, rather than the maths problems used in current encryption. Other techniques could enable early quantum computers to link together and share information in a quantum state. This could increase their processing power and help to secure information. They could contribute to a future network of quantum computers, or a ‘quantum internet’, running parallel to the existing internet.

There are significant technical, engineering and commercial barriers to overcome before different technologies may reach their transformative potential. Nonetheless, they have the potential to unlock scientific and technological innovation across the economy. The previous UK government set out five quantum missions for 2035 and outlined a goal of achieving a “quantum enabled-economy” by 2033 [3]. With such goals, the UK seeks to capitalise on the anticipated benefits and avoid being left behind in the ‘race’ for global science and technology advantage [4].

Our engagement with developments in quantum technologies

Alongside technological developments, there are early ongoing discussions about the future approach for regulating use cases for quantum technologies, based around a responsible innovation approach [5]. We have contributed to this conversation through our work with the DRCF and our most recent Tech horizons report, and wider engagement with bodies such as the Regulatory Horizons Council (RHC) and the Department for Science, Innovation and Technology (DSIT) Office for Quantum.

We are responsible for overseeing the UK’s data protection, privacy and information rights legislation. We regulate the processing of personal information (ie any information that relates to an identifiable living person). This legislation imposes obligations on organisations processing personal information and sets out the rights of people whose personal information they are processing. We have a broad, cross-economy remit that is likely to intersect with some, but not all, applications of quantum technologies.

We support efforts to encourage responsible innovation in quantum technologies by DSIT, the RHC and industry. Compliance with data protection law – including ensuring data protection by design and default – is one of many important factors that will support this. That said, data protection considerations are only one part of a complex national and international picture. As with any cross-sectoral innovation, the emerging landscape is complex and intersects with a wide range of existing regulatory remits.

Our initial work has identified issues where existing data protection regulations are already relevant. It also highlights questions about the intersection of information rights and data protection law, privacy and quantum technologies.

Scope of this report

This report explores quantum technologies, covering future use cases and issues that are relevant to our work. This means those that may involve processing personal information. For that reason, it excludes many other plausible and near-term use cases.

This report explores the following issues:

- Future quantum use cases that may involve or impact on personal information processing, and potential timescales.
- Ways that quantum technologies may converge with other priority technologies we have explored in our previous Tech horizons reports.
- The potential privacy and information rights implications of future use cases. This includes, the extent to which the 'quantum' aspect of quantum technologies may pose novel issues for privacy and information rights, or exacerbate existing issues.
- The future of information security in light of the risks from a quantum computer, and our role in supporting the transition to a "quantum secure" future.

We seek to:

- better understand the technology and landscape, and how existing data protection law may apply now and in future;
- identify opportunities to engage early with industry and set out our regulatory responses;
- identify when and where our voice may be most useful to encourage data protection by design and default; and
- support and contribute to government's broader aim of encouraging responsible innovation in quantum technologies.

We encourage those interested in a wider perspective on quantum technologies and their use cases to refer to the DRCF quantum technologies insights paper ↗r, and websites of the UK's quantum hubs and the National Quantum Computing Centre [6].

Invitation to engage on quantum technologies

This report represents our early stage thinking. We welcome contact from any stakeholders wishing to continue the conversation. Please contact our emerging technology inbox: [email protected].

[3] Department for Science, Innovation and Technology (DSIT) Policy paper on the national quantum strategy missions (2023); DSIT National quantum strategy (2023).

[4] DSIT National quantum strategy

[5] See, for example, Regulatory Horizons Council Independent report on regulating quantum technology applications (2024); Link to the National Quantum Computing Centre (NQCC) responsible quantum industry forum expression of interest; TechUK guest blog by the NQCC on charting the landscape for responsible and ethical quantum computing (2024)

[6] The website of the UK National Quantum Technologies Programme contains links to all of the UK quantum Hubs.

Technologies

This section briefly introduces the range of different technologies that make use of specific quantum phenomena in new ways, what they could do, and how they might be used in future. We focus on those use cases that may involve processing personal information or have privacy and information rights implications. Our list excludes many other plausible and near-term use cases.

Timelines are not predictions, but are intended to reflect plausible futures.

1. Quantum sensing, timing and imaging

Many quantum sensing, timing and imaging technologies are best described as an evolution of existing technologies, offering new or significantly improved capabilities. Potential use cases range across academic research, medical diagnostics, autonomous vehicles, navigation, military and law enforcement surveillance.

Quantum sensors

Quantum sensors make use of specific quantum phenomena to detect and measure tiny physical changes, such as in magnetic fields, gravity and temperature. The 'next generation' of quantum sensors are significantly more accurate and more precise than existing sensors, either offering new sensing capabilities or enhancing existing capabilities [7]. In future, they could be smaller, lighter and more cost effective than current sensors, if hardware improves and technical challenges are addressed [8]. There are examples of investment and pilots across sectors such as the military, healthcare, neuroscience research, civil engineering and environmental monitoring.

There are many different categories of quantum sensor, such as quantum magnetic sensors and quantum gravity sensors. There are also different types of sensor within these broad categories.

- **Quantum magnetic sensors** could be used in various industries, from medical research to defence. For example, some types of sensor can be used for non-invasive, portable and more detailed medical diagnostic tools. This includes wearable brain scanning for epilepsy and Alzheimer's, or diagnosing strokes in a GP surgery. These sensors are able to detect tiny changes in magnetic fields, such as changes generated by individual neurons firing in the brain or by muscle movement [9].
- **Quantum gravity sensors** could be used to detect and map underground infrastructure and hazards (such as pipes or cables) to much greater depths and more precisely than existing gravity sensors can. They could also be used for underwater mapping and navigation. One class of these sensors uses falling clouds of cold atoms to detect tiny changes in the Earth's gravitational field caused by objects or, hypothetically, the presence of people. If successfully miniaturised, they could be used on a moving vehicle, or even a drone, unlike current versions.

Quantum timing technologies

Optical clocks are the next generation of **ultra precise quantum timing** technologies. The time measurements provided by existing quantum clocks (known as atomic clocks) are used for a range of purposes. For example, coordinating high speed online communications or determining location for navigation systems like GPS. Integrating even more precise and compact versions into navigation systems could be used:

- as a faster, more accurate alternative to GPS that is more resilient to jamming by malicious actors. The system could also function better in situations when GPS signal is affected by the environment (such as on a train in a tunnel, or underwater); or
- to enable advanced radar systems to:
  - identify stealth objects or small objects, such as drones, at greater distances; or
  - provide real time location insights and understanding of congested environments [10].

Quantum enhanced imaging

Cameras using novel **quantum imaging** technologies could offer significantly better resolution (detail) and contrast than existing imaging techniques, along with new capabilities [11].

Depending on the type of imaging technique, use cases could include:

- defence and covert surveillance;
- search and rescue or law enforcement cargo scanning to combat human trafficking;
- improving how autonomous vehicles detect and respond to objects in real time; and
- improving non-invasive medical diagnostics and screening for conditions such as cancer.

Researchers have developed ways to give a visible image even in very low light environments, using only a single particle of light. This gives clear images for example, in fog, smoke or underwater. Some techniques can be used to take a picture in infrared using a normal camera, which has applications for biomedical imaging. Others can be used to detect objects and the presence of people around corners, behind walls, or through some opaque surfaces. They use an extremely fast camera to detect scattered particles of light. The next step for many of these techniques is to continue piloting and further refining them for real world applications. Others are far more experimental, such as ‘quantum ghost imaging’ (a technique for taking a picture even when light has not interacted with the object).

Broadly, many quantum sensing, timing and imaging technologies are at a more advanced stage of technical development than other quantum technologies. Some are already in the early stage of commercialisation. Despite significant UK investment for pilots in sectors such as defence, healthcare and infrastructure, there are still some barriers to further adoption, such as:

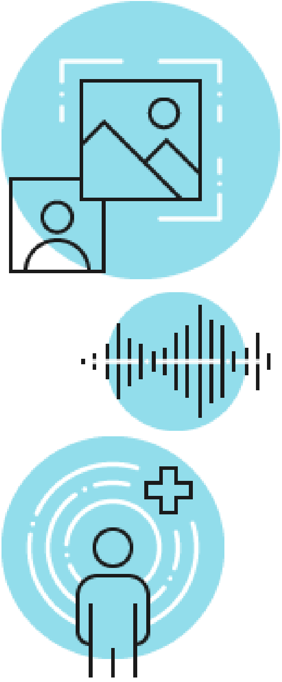
- commercial competition from existing technologies that are already highly effective and widely used. Novel use cases will need to demonstrate that they are fulfilling a specific unmet need [12];
- ongoing technical efforts to reduce size and cost; and
- supply chain challenges.

This means that the future market for many potential use cases most relevant to our remit is still highly uncertain.

Timelines for development of use cases

Current-five years

Increasing academic and military research. Some initial commercial prototypes



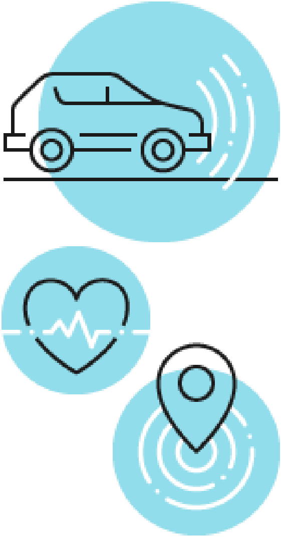
- Prototypes of many sensors and imaging techniques, with some early real-world deployments.
- Ongoing work to reduce their size and introduce commercialised versions.

We could see the following:

- Early real-world deployments of magnetic quantum sensors and quantum imaging techniques in the medical research sector to support mental health therapies and diagnosis of cognitive and other health conditions.
- Ongoing experimentation for underground surveillance, voice detection at a distance, and detecting the presence of people using high resolution ghost imaging in the defence and national security sectors.

Five-10 years

Timescale and potential market for use cases outside healthcare and military highly uncertain over next five-10 years



- In the medical sector, the UK is aiming for every NHS trust to have access to quantum sensing systems for early diagnosis by 2030. Stakeholders suggest this may be difficult to achieve, but we could see magnetic quantum sensors for brain imaging or advanced quantum imaging technologies deployed in some hospitals for more accurate and portable diagnostics of conditions, such as epilepsy or heart conditions.
- Advances in defence applications of quantum sensing and imaging could start to extend into wider civil applications. For example, we may see real world pilots of surveillance devices integrating quantum sensors for high risk law enforcement, search and rescue or hostage recovery applications. For example, handheld sensors to detect concealed weapons at range that ignore other items, or larger imaging systems for detecting the presence of people after a flood or building collapse.
- Increased integration of optical clocks into existing global navigation satellite systems (GNSS) and GPS (ie the systems that enable real time location).
- At the far end of the timescale, quantum imaging technologies integrated into autonomous vehicles to improve how they identify and respond to obstacles.

10-15 years

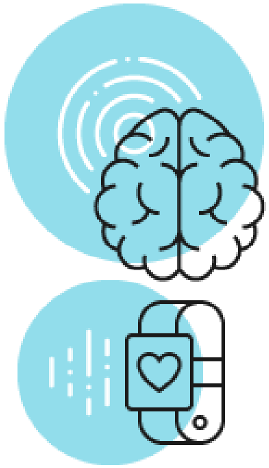
Timescales and potential markets still highly uncertain. If pilots and initial applications are commercially and practically successful, we could see wider uses of quantum sensing and imaging techniques in addition to or instead of classical technologies

We could see the following:

- Tests of quantum sensing, timing and imaging technologies in smart buildings and smart city infrastructure. For example:
  - measuring energy consumption;
  - coordinating information transfers between devices (timing);
  - monitoring real time traffic; or
  - detecting temperature density in populated areas such as shopping malls (to measure shopping habits).
- Quantum imaging capabilities may be integrated into new types of CCTV or drones.
- Certain quantum sensing and imaging techniques used in some GP surgeries or ambulances for portable diagnosis of fractures or heart conditions.

15-25 years

Potential wider integration (eg in healthcare and surveillance)



We could see the following:

- Small, portable and reliable advanced magnetic quantum sensors integrated into various high-end consumer applications and wearable prescription devices. This includes health tech wearables that offer more precise measures of cardiac health, muscle responsiveness and neurological health.
- Wider adoption of certain quantum sensors in applications, such as brain-computer interfaces, when combined with advances in our understanding of the human brain.
- Optical clocks used to coordinate networks of commercial drones.

2. Quantum computing

In theory, a fully functional quantum computer could solve certain problems exponentially faster than the computers we use today. This includes some problems that are so difficult and time-consuming for classical computers to solve that they are considered ‘unsolvable’.

They are most likely to only be used for specific computational problems because they:

- are built very differently; and
- solve problems in a different way.

Organisations that do use quantum computing services are more likely to use them alongside existing computers, rather than to replace them. They are expensive and technically complex, so organisations are also more likely to use quantum computing services through the cloud. At least at this stage, the cost of accessing quantum resources is one of the barriers to wide-scale use [13].

As discussed in further detail later in this report, quantum computing also has well-documented impacts on certain types of encryption and future information security [14]. We are interested in the ongoing efforts to address the risks to personal information that quantum computing may present.

Quantum computers make use of particle behaviour at an atomic or subatomic level to run computations. Classical computers (the computers we use today) process information represented as sequences of 1s and 0s (called digital ‘bits’). In contrast, quantum computers use quantum bits called ‘qubits’. Qubits can represent two states at the same time. This means they can be in both a position of 0 and 1, or importantly, somewhere in between. Qubits can be linked in a way that enables them to represent even more states at the same time. The phenomena responsible for this are known as superposition and entanglement. Due to these properties, the processing power of a quantum computer grows at an exponential rate for each extra qubit.

As noted in our most recent Tech horizons report, researchers are still working out which real-world problems may be best solved using a quantum computer. Many potential use cases are still theoretical, including many that could involve processing personal information. There are also significant barriers to overcome before we reach a fully functional quantum computer, also known as a “universally fault tolerant quantum computer”. It is even possible that we may never reach “quantum advantage” for some use cases (eg if classical machine learning overtakes quantum advances).

Many early anticipated use cases are unlikely to involve processing personal information. For example, using a quantum computer to solve a materials science or physics research problem. Therefore, they would not fall within the scope of data protection legislation. However, researchers and industry are exploring potential future use cases that include the following:

- **Factorising very large numbers**, which has implications for long term information security. Factorising underlies many existing encryption algorithms that protect digital information and communications.
- **Modelling highly complex systems and simulating new chemicals**, which offers possibilities for advances in areas like drug discovery and development and personalised medicine.
- **Solving hard optimisation problems (ie problems that involve identifying the best option from multiple combinations)**. For example, in order to optimise workforce scheduling.
- **Accelerating machine learning** or **improving data analysis** for applications such as:
  - genomics;
  - biometrics;
  - natural language processing;
  - analysing and predicting customer behaviour for product targeting;
  - improving fraud detection in real time transaction information; and
  - classifying images, such as medical scans for diagnostics.
- **Increasing search speed** within complex datasets, or **speeding up the systems used to recommend** products and content on online shopping or media platforms.

Depending on what the computer is being used to calculate, the quantum computer may be processing personal information. Or, the outcome of its calculation may be applied to classical personal information and used to generate insights.

Researchers are also exploring different ways that quantum technologies could be used as, or combined with, classical privacy enhancing technologies (PETs) in future. There is research into:

- **hybrid quantum computing** to improve the computational efficiency of certain PETs [15];
- **federated quantum machine learning**, which would allow a group of organisations to process sensitive information (such as special category data) individually using a quantum computer, and share insights (but not the raw information) with a combined classical model to improve it; and
- **blind quantum computing**, which offers a person or organisation accessing a quantum computer from the cloud, a different way to completely hide the problem they are solving, the calculation, and answer from the quantum computing server (and the organisation that provides the quantum computing service).

Timelines for development of use cases

Current-five years	Noisy intermediate-scale quantum computers (smaller scale prototype computers) and experimentation phase [16]. Prototype versions of quantum computers are already available via

the cloud for research purposes and industry testing.

Partnerships with companies and quantum computers available for public to access remotely for very short periods of time

We could continue to see the following:

- Research and pilots of hybrid quantum-classical applications that use existing quantum computing resources to identify potential improvements on classical AI, and machine learning approaches that will deliver value for commercial applications.
- More pilot projects focusing on hybrid quantum-classical applications in sectors such as financial services, retail healthcare, and life sciences. For example, certain organisations may experiment with using a quantum computer via the cloud as part of a process to:
  - optimise workforce timetables or digital marketing;
  - allocate energy resources to households;
  - personalise financial products; and
  - optimise customer financial portfolios, or customer profiling that takes into account a wider range of factors than is currently possible.

Other experiments include:

- computer vision (which involves searching through large volumes of images to recognise pictures, such as medical images); and
- exploring whether quantum natural language processing, a type of machine learning, could one day help machines understand and use language in a way that is more consistent with how humans use language, for advanced future chatbots and virtual assistants.
- Ongoing exploration of whether adding quantum capabilities to a classical datacentre could improve the efficiency of the datacentre to help it process ever growing volumes of information.

Five-10 years

Mid-scale quantum computers (1000 or more qubits) may begin to demonstrate quantum advantage for certain real world applications (eg improving machine learning)

- If UK capabilities improve and experimentation and pilots increase in the public and private sector, we are also likely to see new applications emerge. For example, in the financial sector, relevant use cases could include using advances in quantum machine learning to improve credit scoring or fraud detection.
- Five-10 years is the earliest projected timeframe for a cryptographically relevant quantum computer to emerge, but predictions are highly varied (five-30 years or more).

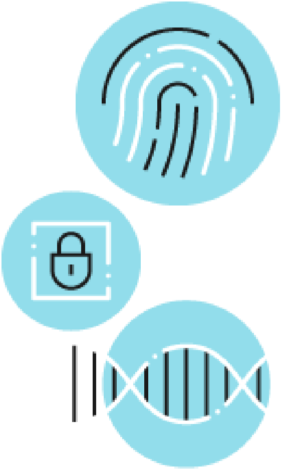
10-15 years

By 2035, the UK is aiming for a sufficiently advanced quantum computer capable of demonstrating high impact in sectors such as healthcare and finance

- For example, in the healthcare sector, this could include adopting hybrid approaches to accelerate analysis of genomic data, or accelerating diagnostics from medical images.
- Depending on the development of quantum computing hardware and software, blind quantum computing could become viable for business-to-business use. It could also be possible that we see early devices for people to use to set up a 'secure' channel to a quantum computer. In tandem, we could see a push for access controls on quantum computers over this period.
- Post-quantum cryptography: The United States (US) has recommended that all critical public systems are upgraded by 2035. The European Union (EU) has recommended member states outline a roadmap to ensure transition "as swiftly as possible". The UK has not set a date for expected transition.

15-25 years or more

Universal fault tolerant computers (computers sufficiently powerful and reliable for a wide range of real world applications)



We could see developments that include the following:

- Computers sufficiently powerful for a wide range of real-world applications, and wider integration of quantum computers into an organisation's computing systems. Many of the potential use cases are yet to be imagined. Some estimates suggest such computers could arrive within 10-20 years.
- Currently highly speculative uses of interest to us include:
  - **polygenic risk scoring** [17];
  - biometric data analysis;
  - using federated quantum machine learning as a privacy enhancing technique;
  - personalised diagnostics;
  - modelling neural activity in a digital twin of the brain;
  - real time credit scoring; and
  - analysing customer behaviour from financial transactions and social media behaviour.
- PETs built for quantum computation may also become viable during this time, such as:
  - federated quantum machine learning;
  - quantum differential privacy; and
  - quantum-enhanced secure multi-party computation.
- We may see the emergence of quantum databases that allow information (eg video, images, music or text) to be stored, organised and queried while still in a quantum state.

3. Quantum communications

There are ongoing UK testbeds and trials of quantum communication networks as an additional way to address the risks to encryption posed by a future quantum computer. Proponents argue that quantum communications will complement the security provided by other techniques, such as post-quantum cryptography [18].

Quantum communications refers to ways of transmitting information securely using quantum mechanics [19]. The main technique is known as **quantum key distribution (QKD)**, a way of securely sharing encryption keys. QKD uses the physical properties of light in a quantum state, rather than using maths problems for security (as in classical encryption). Essentially, sharing the key is secured using the laws of nature [20].

Some suggest that in future QKD could be used together with post-quantum cryptography. This would help protect highly sensitive information transfers against a future quantum computer capable of solving the mathematical problems used in certain types of encryption [21]. It could secure a range of devices, systems and personal information processing, from securing mobile two-factor authentication for online banking to smart buildings and wider digital communications [22]. However, QKD is not currently endorsed by the NCSC for future post-quantum security.

Some stakeholders suggest that QKD is already technically viable. For example, the Quantum Communications Hub have operated a testbed UK quantum network for many years. BT and Toshiba are trialling a commercial QKD network in London. Some other countries are also experimenting with, or have rolled out, QKD networks.

Despite this progress, there are several hurdles in the UK to overcome for further development, such as:

- the cost of implementing QKD networks;
- levels of government and industry demand; and
- appetite to invest.

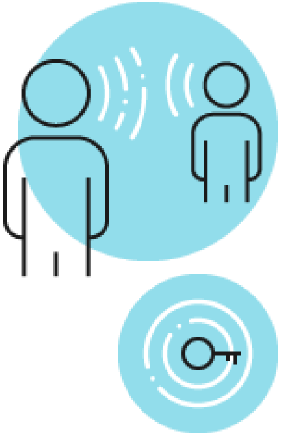
Hardware and engineering limitations also mean that quantum information can currently be transmitted across and between UK cities (up to 100km), but not internationally [23].

Beyond QKD, in the medium term, researchers also hope to link together smaller quantum computers in different places into a more powerful quantum computer. This also opens up the much longer-term possibility of a future national and international network of quantum computers, referred to as a "quantum internet". This would run alongside the classical internet to securely send and receive information in a quantum state (eg qubits), which current networks cannot do. The quantum internet could also be used to send information still in its quantum state from a quantum sensor network (such as in a smart city) to a quantum computer for analysis [24].

Research into linking quantum computers together is still in the early stages of development. As a first step towards a quantum internet, researchers are currently exploring other ways to securely transmit information in a quantum state rather than as classical information [25]. The Quantum Communications Hub is also exploring ways to link quantum computers together. Furthermore, in 2024, UK researchers linked several networks together in a single quantum state for the first time [26].

Timelines for development of use cases

Current-five years



- BT and Toshiba already have a commercial quantum key distribution (QKD) trial ongoing in London.
- Wider uptake will depend on factors such as government and industry appetite to invest in the hardware and network implementation.
- We may also see additional pilots of quantum key distribution (QKD) for high-risk commercial applications, such as telecommunications networks, finance and healthcare. In such cases, QKD could be increasingly offered as an 'extra' for an additional fee.

Five-10 years

- If QKD takes off, we may see progressive bolt ons of QKD, a wider QKD network and increasing use of QKD, (eg for government systems). We may see satellite-based QKD between countries that cannot be supported by fibre.
- We may also see reliable assurance mechanisms in place that help provide confidence to organisations implementing QKD.

10-15 years

- We could see early QKD for consumer devices (eg smartphones).
- The UK aims to link quantum computers together at a small scale by 2035. Depending on the development of quantum computers, we may see initial commercial pilots of networked quantum computers by the end of this period. Developments here may also support improvements in QKD, making security easier to certify.
- We may see some overseas examples of drones used as part of civilian QKD networks. Countries such as the US and China are already experimenting with military applications, but to date the UK has focused on using satellites and existing fibre optic telecoms networks.

15-25 years or more

- Depending on the development of quantum computers, we may see a wider national and international network of quantum computers and blind quantum computing using secure quantum channels to share information.
- At the far end of the timeline we may see emergence of the quantum internet.

Further reading

- UK National Quantum Technologies Programme strategic intent paper 2020
- Department for Science, Innovation and Technology (DSIT) Policy paper on the national quantum strategy missions (2023)
- Website for The Quantum City
- Quantum Delta NL Centre for Quantum and Society exploratory quantum assessment
- EY quantum readiness survey 2022
- GESDA radar: Quantum sensing and imaging
- Website for the UK Quantum Technology Hub in Quantum Enhanced Imaging
- UK National Quantum Technologies Programme article: Look around corners with the quantum periscope
- Nature Perspectives article on Non-line-of-sight imaging (2020)
- Quantum computing for finance: State of the art and future prospects
- German Federal Office for Information Security article: A study of implementation attacks against QKD systems
- APS Physics article: Quantum drones take flight (2021)

[7] 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)

[8] For example, interference from the external environment in real world use cases currently impacts on the accuracy of the measurements.

[9] See, eg, Cerca Magnetics website introducing their brain imaging system based on optically-pumped magnetometers (known as an OPM-MEG System); Quantum Sensing and Timing Hub webpage on sensing the brain

[10] UK Quantum sensing and timing hub webpage on pinpointing the exact location

[11] Cureus article on the quantum-medical nexus: Understanding the impact of quantum technologies on healthcare (2023)

[12] IEEEAccess research article on Exploring quantum sensing potential for systems applications (2023)

[13] techUK report on Quantum commercialisation: Positioning the UK for success (2022). In the short term, accessing them is likely to involve at least some access to overseas quantum computing capacity, as the UK continues to scale its domestic infrastructure.

[14] Specifically, it could be used to solve the mathematical problems that are used in some common types of encryption. See, eg NCSC whitepaper on preparing for quantum-safe cryptography (2020)

[15] Such as **fully homomorphic encryption**.

[16] These **machines** are mid-scale working quantum computers with 50-100 or more qubits. They are prone to errors. They are a step on the road to a fully functional quantum computer that exceeds the performance of super computers and can be used for experimentation and demonstrating some early capabilities. See, eg, DRCF quantum technologies paper and Article by John Preskill on quantum computing

in the NISQ era and beyond (2018)

[17] Polygenic risk scores look at the potential impact of many genomic markers to estimate “an individual’s genetic risk for some trait” or disease. Nuffield Department of Population Health article from the Frontiers journal on calculating polygenic risk scores (PRS) in UK Biobank: A practical guide for epidemiologists (2022)

[18] **Post-quantum cryptography** is a new type of classical encryption believed to be resistant to the known risks posed by a future quantum computer - that is, the ability to factorise large numbers and undermine some types of existing encryption.

[19] Quantum Communications Hub webpage on the background to quantum communications technologies

[20] More specifically, the key is sent as a quantum light pulse, which changes when measured. So, any attempt to copy, intercept or eavesdrop when sending the encryption key would introduce detectable errors. Quantum Communications Hub article on quantum key distribution. QKD is however susceptible to what are known as implementation and side channel attacks: German Federal Office for Information Security article: A study of implementation attacks against QKD systems.

[21] This is known as a **cryptographically relevant quantum computer**.

[22] See eg, Quantum Communications Hub: What does QKD mean for the economy?; Quantum Communications Hub: Consumer QKD

[23] Efforts are ongoing to use satellites to allow communication over longer distances.

[24] University of Chicago News article on the quantum internet, explained; IET Quantum Communication article on the quantum internet: A synergy of quantum information technologies and 6G networks (2023)

[25] IET Quantum Communication article on the quantum internet: A synergy of quantum information technologies and 6G networks (2023); DRCF Quantum Technologies Insights Paper

[26] Imperial College London news release ‘Crucial connection for ‘quantum internet’ made for the first time’ (2024)

Future of information security and the transition to quantum secure systems

The impact of a future quantum computer on certain common types of cryptography is the most significant privacy concern presented by quantum computing. Without appropriate mitigations, a sufficiently powerful quantum computer could undermine the cryptography that protects the security, integrity and confidentiality of almost all private communications and information in transit [27]. This includes personal information. But there are also wider risks beyond our remit, such as to critical national infrastructure, classified intelligence and intellectual property.

A sufficiently powerful quantum computer could be used to solve the mathematical problems used in **asymmetric cryptography**. This type of cryptography is used throughout IT systems and internet infrastructure. Organisations would not be able to rely on this cryptography to protect the future security, integrity and confidentiality of information anymore. There is also a risk that ‘malicious actors’ are harvesting highly valuable and sensitive encrypted information now in order to decrypt it when they get access to a sufficiently advanced quantum computer in the future. This is called a “harvest now, decrypt later” attack.

There is a lot of uncertainty about when such a sufficiently powerful quantum computer could emerge. It could be anywhere between five to 30 or more years away. But, to ensure communications remain safe in the short and long term, there are well-established ongoing efforts to transition to new quantum secure approaches. The main technique is **post-quantum cryptography (PQC)**, which is endorsed by the NCSC.

Efforts to transition, or prepare for the transition, to PQC are accelerating. In particular, we are already seeing:

- examples of implementations in government and industry; and
- technical guidance to support the transition.

The US National Institute of Standards and Technology (NIST) released the first three PQC standards in August this year. The transition may take some time and implementation is likely to be an ongoing process, as with the introduction of any new cryptography standard. For some organisations, it may be as simple as a software update. For others with more complex IT infrastructures, it may be long and costly. Continuing to protect against both current and future cyber threats to personal information will continue to be important. For example, through basic cyber hygiene and keeping cryptography under regular review.

This section further explores the following key questions:

- What personal information may be at risk?
- Where are we now in the transition to quantum secure systems?
- How might the landscape develop, and what might the future ‘state of the art’ of quantum secure processing look like in 10 years?
- Given existing initiatives, what is the ICO’s remit and role in the transition? And what should organisations do?
- What challenges might organisations face during the transition that impact on personal information?

What personal information may be at risk?

Asymmetric cryptography helps protect almost all internet communications, including a wide range of personal information transfers. For example:

- Secure messages, such as emails and encrypted phone messaging services.
- Browsing information or information submitted on secure websites (ie websites protected by HTTPS). For example, when a person accesses government services online, such as benefits applications, e-voting, or passport controls.
- Information that an organisation or person sends to, or accesses from, the cloud. For example, large amounts of information processed for machine learning and data mining, or health information sent between a network of healthcare providers.
- Information sent when using a virtual private network (VPN). For example, when employees are working from home.
- Encrypted information sent by internet of things (IoT) devices. For example, sensor information, video or voice information processed by smart buildings or in smart homes.
- Encrypted information sent by autonomous vehicles, mobile phone apps (eg mobile phone ticketing), or ATMs.
- Financial transactions, online transactions and digital identity schemes.
- In some cases, information held on some blockchains and digital currencies [28].

Asymmetric cryptography is also used for authentication. For example, using a digital signature to prove who a person is on a network, or establishing that a transaction or software download is authentic, such as anti-virus. If a compromised device or user is granted access to a network via one of these routes, they may have opportunities to set up multiple different types of cyber attack.

Identifying and prioritising the information, systems and cryptography that is 'most' at risk is likely to be an ongoing challenge. In general, very high value information that will remain relevant for a long time is considered more at risk than others [29].

The transition to quantum secure systems: where are we now?

There has been a lot of work on ways to address the threat posed by quantum computing. This includes developing new types of "quantum resistant" cryptography (ie PQC), for example:

- The UK government has already introduced mitigations for many critical information and services [30].
- Several bodies, including the NCSC, have developed technical guidance and set out expectations for system owners and large organisations on how to approach the transition [31]. NIST are also developing automated tools to help organisations identify and locate cryptography that are 'at risk' in their systems.
- The US government has set objectives for a public sector transition to quantum secure systems by 2035. The European Commission has also called for member states to develop a road map [32].
- Some web browsers, online messaging and cloud services, and organisations in health and finance have been exploring and implementing quantum secure technologies.

How might the landscape develop, and what might the future "state of the art"

of quantum secure processing look like in 10 years?

Following the introduction of NIST standards in 2024, we anticipate growing uptake of PQC across a broad range of industries in the UK, Europe and the US. Drivers are likely to include international standards, UK government policy, rollout by major service providers, and NCSC guidance. The voice of regulators, including the ICO, will also have an important part to play.

Much as it is today, updating cryptography is likely to be an ongoing process. For example, we are likely to see new PQC algorithms added to the mix during the rollout, as NIST is encouraging their development. We may also see reports about potential discoveries of new vulnerabilities.

We are also highly likely to continue to see classical cyber breaches that impact on personal information throughout the transition period. Such developments are to be expected, and already occur during updates to classical cryptography. Ensuring crypto-agility and management of emerging risks to systems and personal information will continue to be important.

There are also various other techniques in the developing market (not currently endorsed by the NCSC) that we may see organisations adopt in a "quantum secure future" [33]. For example, proponents of **QKD** argue that it will be a necessary complement to quantum secure encryption, as a "physical" guarantee of security. We may also continue to see examples of organisations using a mix of classical and post-quantum cryptography (also known as **hybrid schemes**), or products offering **symmetric cryptography** for protecting certain systems, such as IoT [34].

Overall, it is likely that most people and small organisations will be unaware of how different techniques are being used to secure their browsing and transactions online, such as post-quantum cryptography and QKD. It will be important for people to update their security settings on their digital devices throughout the period and for organisations to continue to encourage good cyber hygiene. For large organisations, and those that manage their own cryptographic infrastructure, updating their cryptography over the next ten years could be more complex.

What is the ICO's remit and role in the transition?

We are not the only domestic regulator with relevant responsibilities [35], and there are also significant international dimensions to the transition. But, we have a wide, cross-economy remit to support the long-term security of personal information and to oversee compliance with information security obligations under:

- UK GDPR and the Data Protection Act 2018 (DPA);
- NIS, as it applies to cloud services and e-commerce platforms; and
- eIDAS, which applies to organisations that provide digital identity or authentication services.

In our view, organisations should consider identifying and addressing quantum risks as part of their existing legal obligations to adapt to new and emerging cyber threats to personal information.
Under UK GDPR, organisations must process personal information "in a manner that ensures appropriate security of personal data … using appropriate technical and organisational measures." Measures must be appropriate to the risks of processing, and organisations must consider the state of the art [36].
Organisations must also report personal data breaches to us.

Cloud services and e-commerce providers, organisations that provide digital identity or authentication services, and internet and telecoms providers also have security obligations under NIS, eIDAS and the Privacy and Electronic Communications Regulations (PECR) respectively. We oversee compliance with these obligations.

There are a range of actions we can take, for example:

- providing guidance, engagement and education;
- assessing and investigating breach reports;
- undertaking proactive and reactive audits;
- issuing information or enforcement notices; and
- in the most serious cases, fining organisations for breaches of their obligations under the relevant legislation.

For example, our role under NIS is to develop guidance and work with the NCSC and law enforcement to respond to security incidents affecting cloud service providers and e-commerce platforms. These may or may not involve personal information. A cloud service would have to report a breach to us as either a NIS incident, or a UK GDPR personal data breach, if they:

- were alerted to a "harvest now, decrypt later" attack that substantially affected their service or led to the disclosure of personal information; or
- made a mistake in implementing PQC that left personal information exposed, that carries a risk to people's rights and freedoms.

We would assess factors such as the impact of the breach and the pre-existing cyber measures an organisation has in place. We would respond proportionately according to our regulatory action policy and our regulatory approach under ICO25 [37]. We would work closely with other competent authorities and the NCSC.

There is a risk that organisations do not adapt to the risks posed by a future quantum computer because of factors such as uncertainty or cost. For other organisations, they may still be working towards a baseline level of cyber security to respond to current and more immediate threats. Alternatively, organisations may rush to implement non-standardised solutions and in doing so inadvertently put personal information at risk.

These are examples where input from the ICO and other regulators could have an important part to play in the transition.

1. Our short term role: guidance, engagement and education

We are committed to supporting organisations to understand current and future cyber risks so that they can appropriately protect personal information. We also support efforts to encourage the transition to PQC, once standards-compliant products are available.

Under the DPA and UK GDPR, it is for organisations to determine what technical measures they need to ensure the appropriate level of security for personal information. Nonetheless, we are committed to supporting organisations to understand current and future cyber risks so that they can appropriately protect personal information.

Our encryption guidance emphasises that organisations should be crypto-agile. This means that they keep their encryption use under regular review and remain aware of updates and vulnerabilities. New standards have been developed and, at some stage in the next 10 years, PQC is likely to become an accepted and widely implemented norm in the future state of the art.

In the UK, there is currently less consensus around other quantum-secure technologies, such as QKD or quantum random number generation. Some commentators suggest that the future improvements to these technologies that are currently being developed will lead to a wider uptake.

Our immediate focus is to support existing efforts to prepare for, and encourage, the transition to standards-compliant PQC. For example, we intend to:

- continue to help raise awareness of the risks posed by a quantum computer and the importance of mitigations; and
- update our existing guidance on the security provisions of UK GDPR to reflect the new PQC standards at a later date, in line with the transition to PQC.

This will support the long-term security of personal information.

As the landscape evolves, so will our approach. We will continue to engage externally and are already using futures methodology to help inform this planning.

2. Timelines for transition

In our early engagement, some stakeholders asked whether we will set an expected date for transition to post-quantum cryptography or develop a roadmap and timeline, as some other countries have done. So far, the UK has not taken this approach. Others are interested in when we may start ‘enforcing’ a transition. We will continue to engage and consider these questions in consultation with relevant stakeholders.

What should organisations do?

Under both UK GDPR and NIS, organisations should “have regard to the state of the art” when considering the appropriate security measures that are proportionate to the risk of their processing.

1. Post-quantum cryptography

Following existing obligations and good practice, large organisations should:

- start considering their risk exposure in the immediate and near future.This could include identifying high risk information, critical systems and at-risk cryptography; and
- refer to evolving international standards and NCSC guidance, as required under existing regulations (NIS and UK GDPR).

2. Classical cyber security

Organisations must also continue to protect against the wide-ranging, short- and medium-term cyber security concerns unrelated to quantum computing. This includes basic, day-to-day cyber hygiene. Poor cyber security and classical cyber attacks continue to pose immediate, significant risks to personal information, and the potential for significant economic and personal harm [38].

For further information on managing day-to-day cyber security, see:

- ICO guidance on security, including cyber security and encryption
- ICO guidance on records management and security
- ICO NCSC joint guidance on technical measures and security outcomes
- NCSC Cyber Assessment Framework

3. Other quantum secure technologies

If an organisation is considering whether to use other quantum secure technologies, such as QKD, in addition to PQC, they may consider completing a data protection impact assessment (DPIA). A DPIA may be required, if an organisation's processing activity is likely to result in high risk to people's rights and freedoms. A DPIA can help an organisation:

- assess risks to people's rights and freedoms associated with their processing of personal information; and
- document measures they are taking to address the risk and their reasons.

It should also be noted that under NIS, relevant digital service providers must also provide adequate documentation to demonstrate compliance with the legislation.

What challenges might organisations face during the transition?

It will be important that we have a good understanding of how different sectors and organisations are progressing with the transition, and the challenges different sectors are facing. While the scale of the transition, and complexity of PQC algorithms is new, we have seen many of these challenges before, in past cryptography transitions.

Some challenges that could arise include:

- **Misconfiguration errors**: Organisations, such as a cloud service provider, might make a mistake when transitioning to PQC that is exploited by a malicious actor, leaving personal information exposed.

  Regulatory implications: If the personal data breach is likely to result in a risk to people's rights and freedoms, the organisation would need to report the personal data breach to us. We would then decide on further action, taking into account factors such as the impact of the breach and the cyber security measures an organisation had in place. We would also engage with the NCSC where appropriate.

- **Complex data processing involving multiple data controllers, data processors, devices and legacy IT systems**: Organisations may want to enter into complex data sharing arrangements. An example would be councils, public and private health providers and law enforcement authorities wanting to share information to deliver better services to at-risk groups. Organisations may be subject to different constraints, such as legacy equipment or limited budgets to transition to a 'fully' quantum secure system. Some may not have a good working knowledge of their existing cyber-security infrastructure.

Regulatory implications: Organisations may need to work together with providers and third parties to coordinate the shift to quantum secure systems. Primary legal responsibility for implementing appropriate security measures rests with each organisation, as data controllers. Data sharing agreements and regular cyber security protocols can support risk management.

- **Diverging international approaches**:International standards are developing, butdifferent countries may choose to adopt different timelines and set out different expectations around which quantum secure technologies to adopt.

  Regulatory implications: Navigating this intersection may be complex for organisations operating internationally, but it must not be a barrier to compliance with UK law. We are committed to working with other domestic regulators to explore the overlap, and with our international partners to maintain an interoperable data protection regime [39]. International engagement on quantum standards is led by the NCSC and DSIT. We monitor relevant developments as an observing member of the British Standards Institute PQC standards working group.

- **Lack of PQC for certain privacy enhancing technologies**: For organisations that choose to deploy certain privacy enhancing technologies [40], it is likely there will be an overlap or delay between implementing classical versions, and the arrival of "quantum secure" versions of these techniques. This could affect, for example, the use of zero knowledge proofs in digital identity or age assurance services. The technique is used to digitally prove something about a person, such as their age, in order to access a service without disclosing the person's actual age.

  Regulatory implications: Organisations will need to consider the impact of quantum computing on privacy-enhancing technologies that they are deploying. In some cases, they may need to adapt their approach pending the arrival of "quantum secure" versions of these techniques. We will continue to monitor the impact of quantum computing on privacy-enhancing technologies.

Further reading

- NCSC blog on post-quantum cryptography: what comes next (2024)
- ETSI whitepaper on quantum safe security cryptography and security: an introduction, benefits, enablers and challenges (2015)
- NIST cybersecurity white paper on getting ready for post quantum cryptography: Exploring challenges associated with adopting and using post quantum cryptographic algorithms (2021)
- CSIRO paper on the quantum threat to cyber security: Looking through the lens of post-quantum cryptography (2021)
- European Data Protection Supervisor's TechDispatch on Quantum Computing and Cryptography (2020) _
- NCSC white paper on quantum security technologies (2020)

[27] NIST video on post-quantum cryptography: the good, the bad, and the powerful; NCSC whitepaper on preparing for quantum-safe cryptography (2020); ETSI whitepaper on quantum safe security cryptography and security: an introduction, benefits, enablers and challenges (2015)

[28] ETSI whitepaper on quantum safe security cryptography and security: an introduction, benefits, enablers

and challenges (2015); CSIRO paper on the quantum threat to cyber security: Looking through the lens of post-quantum cryptography (2021)

[29] NCSC whitepaper on the next steps in preparing for post-quantum cryptography (2023)

[30] DSIT National Quantum Strategy

[31] NCSC blog on post-quantum cryptography: what comes next (2024); NCSC whitepaper on the next steps in preparing for post-quantum cryptography (2023); NCSC white paper on quantum security technologies (2020); NIST article on the release of the first 3 finalised post-quantum encryption standards (2024) ; ETSI technical report on migration strategies and recommendations to quantum safe schemes (2020); Quantum Communications Hub press release on annotated NCSC technology assurance principles relevant to quantum communications (2024)

[32] European Commission recommendation on a coordinated implementation roadmap for the transition to post-quantum cryptography

[33] Other techniques include **quantum random number generation**, and **hybrid cryptography** schemes.

[34] An existing example is ArQIT's cloud-based symmetric key encryption platform.

[35] For example, other competent authorities under the NIS regulations include Ofcom, Ofgem and The Civil Aviation Authority: NIS Guidance for Competent Authorities, Annex A. As noted in the DRCF paper, the FCA imposes a range of obligations that are related to operational resilience.

[36] ICO guidance on data security

[37] ICO guidance on breach response and monitoring; ICO guidance on NIS enforcement

[38] See, eg, ICO media release on the growing threat of cyber attacks and our Learning from the mistakes of others report (2024); ICO data security incident trends dashboard; NCSC and NCA whitepaper on ransomware, extortion and the cyber crime ecosystem (2023), NCSC Annual Review 2023

[39] DRCF quantum technologies insights paper and ICO webpage about our international work

[40] Such as **fully homomorphic encryption** and **zero knowledge proofs (ZKP)**.

Wider information rights issues

From a privacy and information rights perspective, many of the immediately apparent issues associated with applications of quantum technologies are similar to those raised by classical technologies. But, in some cases, the unique physical characteristics of quantum information, and new capabilities, could exacerbate existing privacy and information rights issues, or introduce new issues.

Cross-cutting issues

1. Identifying personal information processing and implementing data protection by design and default

UK GDPR applies to the processing of personal information, which is information that relates to a living person who can be directly or indirectly identified from the information. Organisations that process personal information as part of a use case need to embed privacy by design and default. They also need to consider information governance and individual rights.

Determining whether or not a quantum technology use case involves processing personal information may not always be straightforward. Our Tech horizons report chapter on quantum computing highlighted that uncertainty around future use cases and the types of training data in use can be a complicating factor. Other factors include what algorithm the computer is solving, and the information that algorithm needs in order to work. For uses of quantum sensing and imaging techniques, it could be challenging to identify what information the novel or increased capabilities are collecting, and how this information interacts with other data streams.

These are not challenges unique to quantum - we often provide input on such questions in our Sandbox. But, in future, the novelty and complexity of quantum concepts and technology could be an additional barrier to engaging internal teams on basic data protection questions.

Nonetheless, the data protection approach should not be any different just because a technology is ‘quantum’. Data protection obligations only come into play if the information relates to an identifiable living person.

Taking the example of quantum sensing and imaging techniques, it is not clear whether the following would collect personal information:

- Quantum imaging techniques that can see around corners and detect the presence of a person or object outside the line of sight can, at least at present, generate a low resolution outline of a person moving through a space, and an outline of other objects. See Image A. In this case, it is possible that with advances in machine learning techniques, the data collected could in future lead to far more detailed images. This could mean people are identifiable. Research is also exploring approaches that could, in future, detect things ‘through’ some surfaces such as bone. Information from these techniques could also be combined with other information [41].
- Quantum magnetic sensors may be able to detect the presence of certain objects through walls and people in spaces. The level of detail they can collect is unclear.
- A quantum gravity sensor can map shapes and objects over large areas. At the moment, it might be

able to detect the presence of a person, but nothing more.

Detecting the presence of an unidentifiable person, without more detail, is unlikely to fall within scope of data protection legislation. But, other factors may inform the assessment of whether a person is identifiable, and therefore whether personal information is being processed. For example:

- the context;
- what other information an organisation has; and
- what other processing is taking place (eg is information being combined with information from other sensors being used on the device) will inform whether or not personal information is being processed.

For example, if quantum imaging that can see around corners or behind walls was deployed for directed surveillance, the organisation is likely to have further information that would identify the person. This means that they would likely be processing personal information. If such a device was deployed in CCTV in a public space such as a hospital, the organisation may hold additional information about patients and staff. Therefore, capturing a low resolution outline (as opposed to a detailed image) might involve processing personal information. But this is not clear-cut.

Image A: Quantum imaging around corners or behind walls [42]**.**

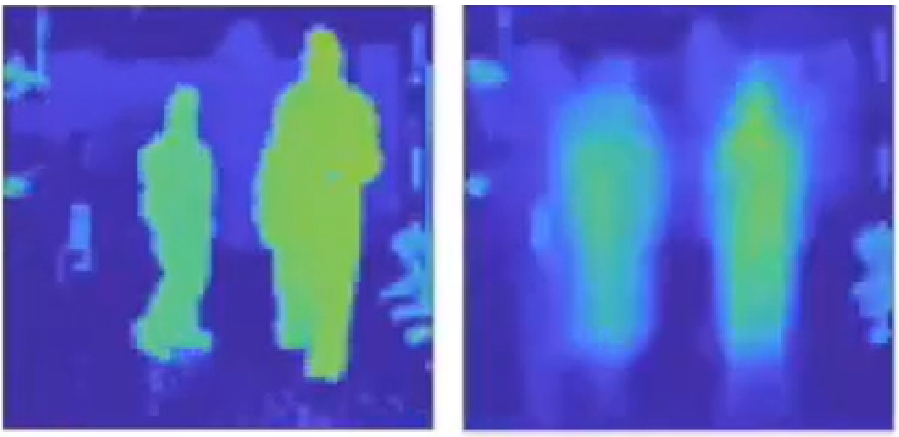
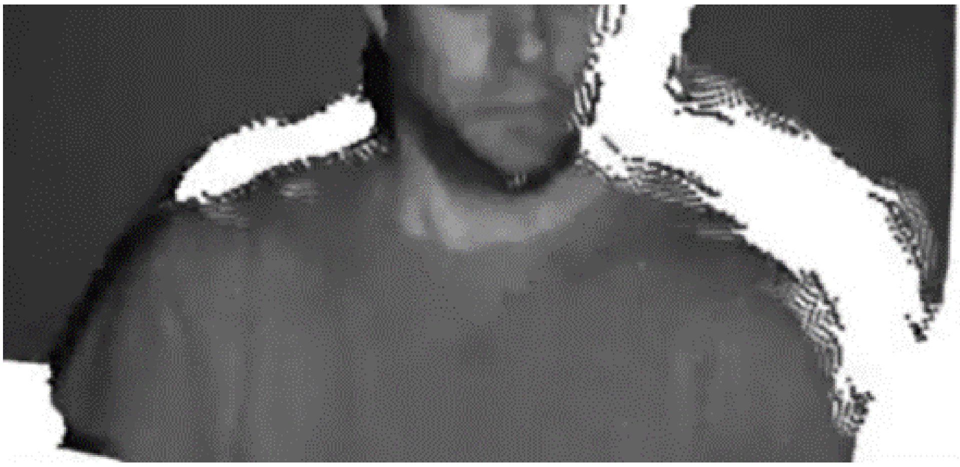


Image B: High-speed 3D Quantum imaging using single particles of light.



In other cases, identifying processing of personal information is likely to be obvious, for example:

- Using a **quantum magnetic sensor** for non-invasive brain scanning or quantum imaging techniques for medical diagnostics. The results of the scan or imaging will clearly relate to the person being scanned.

- Capturing an identifiable person using certain **low light quantum imaging techniques**. The technique generates a detailed 3D image when the information from individual light particles is stitched together using machine learning. For example, Image B, if used to capture a whole face, captures a greater level of detail that appears more likely to involve identifiable information.

In many cases, these technologies may be embedded within a wider system, such as an autonomous vehicle or robot. What is important is that organisations deploying these technologies, or systems using these technologies, have a full understanding of:

- what information the sensor or camera can collect;
- how they are going to use the sensor or camera (and system); and
- what other information they may have or be able to access (eg information from other sensors or inferences from machine learning).

This will help them to:

- identify whether they are processing personal information;
- unpack what the potential impacts may be on people's rights and freedoms; and
- take appropriate action.

A DPIA is a useful starting point.

Quantum sensing, timing and imaging issues

1. Risk of surveillance and data minimisation

One concern about the emerging capabilities of quantum sensing and imaging technologies is that they could open further avenues for overt or covert surveillance, or excessive information collection.

In particular, certain techniques:

- can collect information in new ways;
- can collect information with even greater degrees of precision, at further distances; and
- in future, could be deployed in very small and portable devices.

The capabilities could be:

- useful in law enforcement (eg to detect at a distance whether someone is carrying a weapon or a weapon is in a building);
- deployed to assist with emergency service recovery or for directed surveillance in national security scenarios (eg to detect objects or movement at a distance or in another building); and
- potentially used to develop certain techniques (such as 360 degree imaging) for CCTV in prisons, hospitals or the home, or to support autonomous vehicle safety.

Some of these use cases could have many benefits. Others could be highly privacy intrusive, even if not processing information about identifiable people. For example, if not deployed and managed responsibly, lawfully, fairly and transparently, such capabilities could open up previously private spaces, such as homes, to unwarranted intrusion. People may also not be aware of, or understand, what information is or is not being collected about them. This can foster mistrust or have a chilling effect on how people behave in public and private spaces. Integrating data protection by design and default provides a robust way to help address surveillance concerns.

Minimising the personal information collected and being transparent about data processing can help increase trust when implementing new technologies that could be used for surveillance.

As noted in the previous section, it is also important to be clear about:

- what new quantum sensing and imaging technologies can and cannot detect; and
- whether or not they materially add any risk to people's rights and freedoms.

In some use cases, the limitations of a particular sensor could even mean that less identifying information is collected than classical alternatives (eg CCTV).

For example, future autonomous vehicles are likely to rely on a range of different sensors and ultra precise timing and navigation technologies to safely interact with their environment and anticipate obstacles. Next generation quantum imaging and timing technologies could be deployed to further improve these capabilities. For example, by enabling a 360 degree view of the environment and obstacles around corners, in real time, even in low light, fog or very cluttered areas [43]. It is still unclear whether they could also capture detailed information about a person's route home or their neighbourhood. But autonomous vehicles are already likely to collect location and other information, whether quantum technologies are used or not. Any additional data protection risk is likely to be cumulative and also depend on an organisation's information management practices.

2. Use for national security, intelligence and law enforcement purposes

Use of covert surveillance or other covert investigatory powers by public bodies is covered by the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA). The Investigatory Powers Commissioner's Office, not the ICO, provides independent oversight of the use of all investigatory powers by intelligence agencies, police forces and other public authorities. However, whether such activities are legal under RIPA and IPA will also influence if any associated processing of personal information is lawful under data protection legislation.

But no matter what application or technology is used, organisations processing personal information for national security, intelligence or law enforcement related purposes, still need to comply with the applicable data protection regime, whether that is UK GDPR or Part 3 (Principles - Law Enforcement Processing) or Part 4 of the DPA18 (and Principles - Intelligence Services Processing). This will also apply to relevant future uses of quantum sensing, timing and imaging technologies in these settings.

The data protection legislation provides exemptions which are applicable to specified provisions. For example, an organisation may seek to rely on an certain exemption where required to:

- safeguard national security; or
- avoid some form of harm or prejudice, such as impacting on the combat effectiveness of the UK's armed forces [44].

But none are blanket exemptions. In each case, the processing must also still be lawful (eg it may be subject to a warrant, or Ministerial authorisation). An organisation seeking to rely on the exemption also still needs to comply with their accountability and security obligations [45]. Organisations that may often rely on exemptions should also regularly review their processing to avoid expanding the scope of the processing unnecessarily (also known as “scope creep”).

Quantum computing issues

1. Accuracy, fairness and explainability

Data protection law sets out an obligation for organisations to take reasonable steps to ensure personal information they process is accurate (ie not misleading as to any matter of fact). The outputs of many machine learning systems are not facts, they are “intended to represent a statistically informed guess” about something or someone [46].

Much like many machine learning models, quantum computers are probabilistic. This means that they will give the “most likely” answer, rather than a definitive one. Calculations on current quantum computers are also prone to errors, because qubits are fragile and impacted by interference from the outside world (noise). This fragility does not introduce inaccuracies - it stops the whole computer from working. But, verifying the accuracy of quantum calculations is very complex, and technical explainability frameworks for quantum machine learning have not been developed yet.

If an organisation makes an inference about a person using the output from a quantum computer, the inference does not need to be 100% accurate to comply with the accuracy principle. The organisation needs to record details such as:

- the fact the inference was made as a result of an analysis by a quantum computer;
- the inference is a “best guess”, not a fact; and
- relevant details about the limitations of that analysis.

But, the accuracy of the system’s output (we call this **statistical accuracy**) is relevant to an organisation’s fairness obligations.

If an organisation wants to rely on an inference from a quantum computing output to make a decision about someone, they need to know that the calculation and the inference is sufficiently statistically accurate for their purposes. The calculation needs to be “sufficiently statistically accurate to ensure that any personal data generated by it is processed lawfully and fairly.” [47] Under the fairness principle, organisations should handle personal information in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

At the moment, it is possible to test statistical accuracy and demonstrate whether quantum computing calculations are more accurate than equivalent classical models using existing classical computing methods. However, in future, it is not yet clear how to assure and demonstrate computational accuracy, especially to a non-expert, once quantum computing capabilities sufficiently outstrip those of a classical computer. For example, if it would take a classical computer decades to solve the problem) [48]. This is still an active area of research.

This could potentially pose some challenges for organisations to comply with their fairness obligations, depending on what they are using the quantum computer for. It could be relevant for specific use cases that may involve processing personal information that is likely to result in a high risk to the rights and freedoms of natural persons (**high risk processing**), where the accuracy of inferences cannot be confirmed without additional investigation. For example, using a quantum computer to detect fraudulent transactions in a complex dataset, or drawing inferences from genomic information. Organisations would need to record these inferences as an opinion.

In such cases, even if the dataset is accurate, there may not always be information available that could ‘prove’ a transaction was fraudulent, or that the inferences made are correct, without further investigation. But, in future, an organisation may intend to take decisions automatically on the basis of the quantum computing analysis (eg, to automatically freeze an account or refuse a credit application). In that case, maximising (and understanding) statistical accuracy becomes very important to ensure fairness.

At the moment, current quantum computers are mainly used to accelerate existing machine learning algorithms. The state of the art and use cases continue to evolve and research continues into assurance and verification. Organisations must ensure they understand and document the limitations of the systems they are using. They must only use systems that are sufficiently statistically accurate for the intended purpose.

2. Transparency, storage and retention

The nature of quantum information is very different to classical information. At the moment, qubits do not last very long because their state ‘collapses’ when observed, measured, or when they are affected by the outside world. They cannot be copied and are currently fragile and prone to errors that collapse the computation.

These physical properties are not features of information in classical computing.

Following on from questions raised in the Tech horizons report, we have explored whether these physical properties of qubits may:

- have implications for an organisation’s data protection obligations; or
- make it harder to fulfil people’s rights in a quantum-enabled future.

For example, we have considered whether:

- the organisations running a quantum computer are still processing personal information if a computation collapses. If the organisation is not, it would no longer have data protection obligations over that information;
- it will be possible, in future, to store quantum information and correct any inaccurate stored quantum information about a person; and
- organisations need to (or are able to) respond to subject access requests if using a quantum computer or hybrid quantum-classical approach to process personal information, and the computation collapses.

From a technical perspective, initial engagement suggests it is still very early days to be considering these questions and they are underexplored. They are only likely to become relevant in the far longer term (10-25 years or more), if we reach the era of universal fault tolerant computers. By that point, some of these questions may have been addressed by anticipated technical developments. There are several reasons for this:

- **Increasing stability of qubits**: It is anticipated future qubits will be more stable and not introduce the errors they do today [49], some of these issues are less likely to be relevant. Advances in error correction will mean that the information being processed will be spread between qubits. Error correction could be applied at each stage of computation. If there is an error in any one qubit during part of the computation, that error could be corrected without the whole computation collapsing.

- **Current and future storage of quantum information**: There are not yet reliable ways to store quantum information at scale, for later processing.There are theoretical approaches, but researchers need a larger quantum computer (with more qubits) to implement them. In the short term, if a quantum computer is used to process personal information, data protection principles apply when the processing is proposed and as it is being carried out. The computation may be run multiple times. But, the organisation is not storing quantum information. Therefore, questions do not yet arise about correcting stored personal information or answering subject access requests about any information "held" by a quantum computer. Any decisions an organisation makes about a person as a result of processing by a quantum computer would still be subject to data protection obligations.
- **Classical information is converted into quantum information prior to processing**: In order to use a quantum computer, classical information needs to be described and transformed (encoded) into a quantum state. Once the computation is complete, it needs to be encoded back to classical information again, to give an answer that can be read by a classical computer. Even if a quantum computation collapses, either the controller or processor is likely to still hold and be processing classical information that they would need to disclose in response to a subject access request.

3. Blind quantum computing, privacy, and harmful processing

For the foreseeable future, people and organisations are likely to access quantum computers remotely, via the cloud. UK researchers are exploring a technique called blind quantum computing. This could add a further layer of security and privacy protection for highly sensitive information processing when using quantum computers. This could include anything from commercial secrets to processing special category data, such as health or genetic information [50].

In the long term (10-15 years), this technique would enable a person or organisation to run an algorithm, get an answer, and verify their results, without the quantum computing cloud server being able to see what they were doing. Their processing would be hidden in a way that was 'assured' by quantum physics [51]. More specifically, qubits collapse when measured. Therefore, any attempts to copy, intercept or eavesdrop on the communication or processing on the server would collapse the quantum computation or the communication channel, so the information cannot be read [52]. If the technique takes off, it could even lead to plug-in devices for people wanting to use quantum computing cloud services from home, with 'guaranteed' privacy [53].

Proponents have speculated that this technique could help further enhance the security and privacy of processing using a quantum computer. For example, stakeholders have speculated whether it could be a future way of securely processing sensitive personal information, such as special category data, using quantum computers in other countries, to satisfy UK GDPR rules about transferring information internationally. Whether this is the case, is a question for us to consider further.

Others have highlighted that the technique may also create new challenges for counteracting attempts to use a quantum computer to enable certain types of malicious and criminal activity online. Such potential malicious use cases are extreme scenarios. However, they do raise questions about the balance to be struck between the privacy benefits of blind quantum computing, and the harms that could arise from serious misuse of blind quantum computing capabilities.

From a futures perspective, we may see current concerns about harmful uses play out in a similar way in a quantum-enabled future. For example, we could see emerging discussions around:

- ways to flag dual uses for quantum algorithms, or detect what algorithm a person is wanting to run on a quantum computer;
- proactive scanning for harmful content on a person's or organisation's computer (known as client-side scanning); or
- access controls or identity verification when signing up for access to a quantum computer.

We will need to further explore how this issue may develop, and what our approach might be, in a future quantum-enabled world.

Quantum communications issues

1. Securing QKD networks and access to QKD nodes

Pilots of QKD networks are exploring ways to offer future secure communications to help address the risks from a future quantum computer. Researchers are also exploring ways to integrate post-quantum cryptography into QKD networks to help develop 'end-to-end' encrypted communication networks [54]. This is distinct from blind quantum computing above, as it involves securing information sent through the regular internet (as per chapter four), not just protecting information when accessing a quantum computer.

Our early research suggests the way these networks are set up could also lead to privacy concerns, if not appropriately managed. At the moment, quantum information (such as encryption keys) can be transmitted up to 100km away. The information is transferred between physically secured trusted nodes operated by internet service providers, until it reaches the final destination [55]. It is not yet possible to transmit information at longer distances, or internationally, but efforts are ongoing to use satellites for this.

Quantum communications experts noted that it could either create a secure link:

- between two customers; or
- between the customer and internet service provider.

The type of secure link will depend on how the technology develops, how a future QKD network is set up and how it is deployed with PQC.

The first setup is similar to classical end-to-end encryption. Only the intended recipient could decrypt whatever is sent. In the second setup, a service provider could, in theory, intercept and decrypt the quantum secure communication at each "trusted node". The second option, theoretically, provides additional points of access to communications for:

- a malicious actor; or
- law enforcement or intelligence services to prevent crime or other online harms. This would need to be authorised under the applicable legislation (RIPA or IPA).

Commentators have suggested that if this second approach is adopted, providers cannot claim to offer end-to-end post-quantum security.

At this stage, it is not clear which approach the UK may adopt, but we are alert to the potential privacy risks of the second approach. We are open to engaging further on this issue, should QKD networks continue to develop.

Existing regulation under RIPA, IPA, UK GDPR and PECR set out obligations for telecoms providers to ensure the security of their services, and for agencies seeking access to communications. For example, PECR regulation 5(1A) states that telecoms providers must "ensure that personal information can only be accessed by authorised personnel for legally authorised purposes". Ensuring that all organisations continue to comply with their data protection and PECR obligations, as well as RIPA, when establishing and running new networks will help maintain people's trust.

Further reading

- ICO guidance: What is personal data?
- ICO guidance on automated decision-making
- Overview of ICO data protection harms and the ICO taxonomy

[41] Nature Perspectives article on Non-line-of-sight imaging (2020); University of Glasgow blog on The nano and quantum world: Extreme light. At the moment, researchers have used the technique to see through up to 5cm of opaque material, such as bone, which they are using to explore brain imaging. Non line of sight imaging could also be combined with information such as the partial information provided by radar and wifi, which can see through certain kinds of wall.

[42] QUANTIC videos on sensing and imaging for defence and security; Image A is from the video on non line of sight imaging. Image B is from the video on real time 3D imaging.

[43] Nature Perspectives article on Non-line-of-sight imaging (2020); Quantum Sensing and Timing Hub article on transforming detection with quantum-enabled radar; Transforming detection with quantum-enabled radar (quantumsensors.org); Transcript of House of Commons Science and Technology Committee oral evidence: Quantum technologies (2018)

[44] See also: ICO guidance on law enforcement processing: National security provisions; ICO guidance on intelligence services processing: Exemptions

[45] ICO guidance on intelligence services processing: Exemptions

[46] ICO guidance on AI and data protection: What do we need to know about accuracy and statistical accuracy

[47] ICO guidance on AI and data protection: What do we need to know about accuracy and statistical accuracy

[48] Quantum Computing and Simulation Hub article on Verifiable blind quantum computing with trapped ions and single photons (2023)

[49] This type of qubit is known as a logical, error corrected qubit.

[50] Quantum Computing and Simulation Hub article on Verifiable blind quantum computing with trapped ions

and single photons (2023) The technique involves a person sending a problem to a universal fault tolerant quantum computer via a quantum link (ie, sending information encoded on particles of light), running the problem and receiving the answer to a device attached to a computer via that same link.

[51] More specifically, it provides information-theoretic security. Quantum Computing and Simulation Hub article on Verifiable blind quantum computing with trapped ions and single photons (2023)

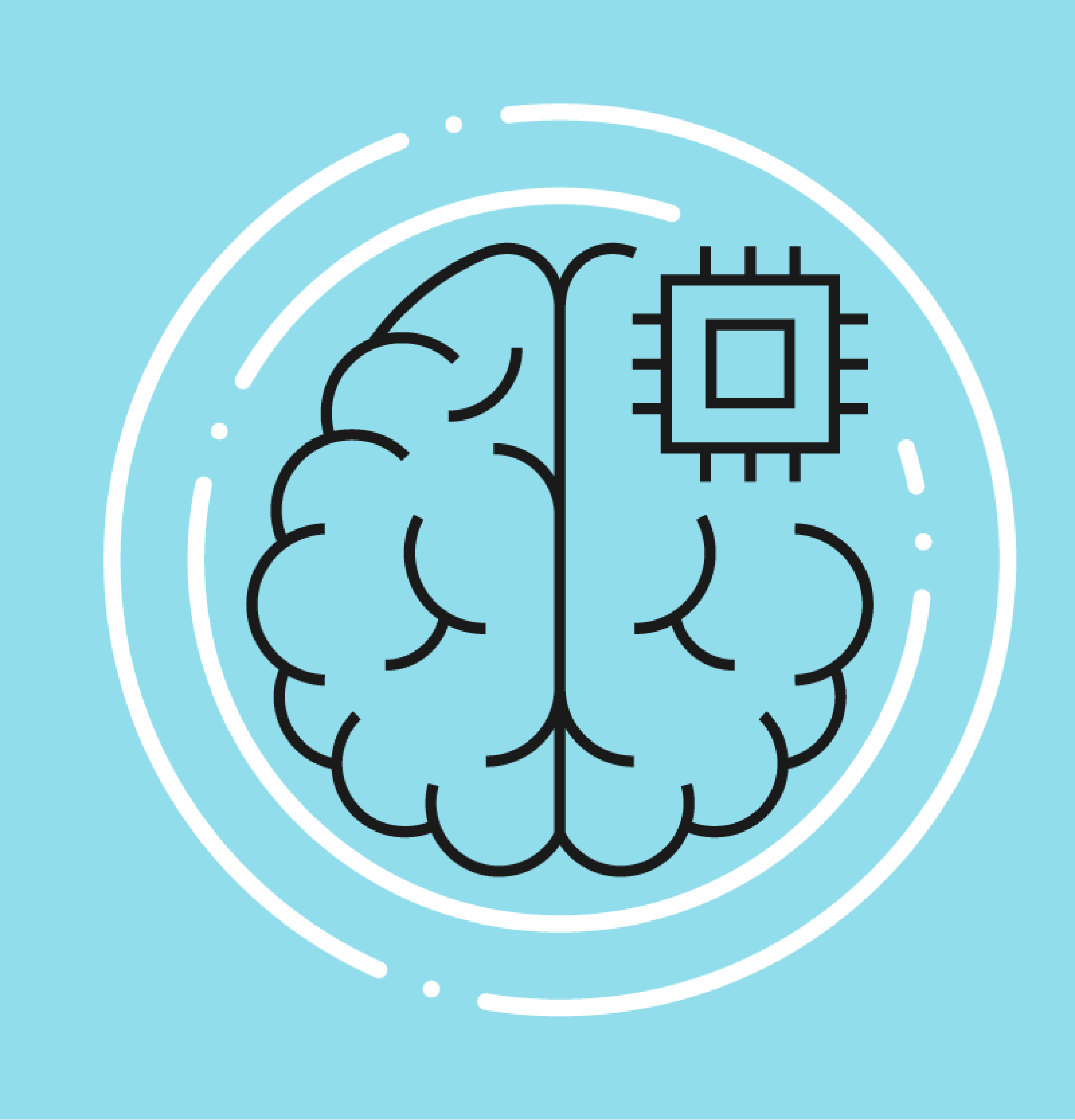
[52] Quantum Computing and Simulation Hub article on Verifiable blind quantum computing with trapped ions and single photons (2023)

[53] University of Oxford media release: Breakthrough promises secure quantum computing at home (2024)

Future connections with other ICO priority technologies

Emerging technologies do not develop in a vacuum. As ‘enabling’ technologies [56], quantum technologies are likely to impact many different technologies, sectors and use cases. Given their early stage of development, there is not yet a clear picture of many potential use cases and their impacts, but there are some early indicators. In this section, we explore some plausible (and some more speculative) ways quantum technologies may influence some of our other priority emerging technologies we discussed in previous Tech horizons reports. We also briefly highlight some of the privacy implications of these developments.

Neurotechnology



There are some near-term neurotechnology use cases for **quantum sensing and imaging** in the healthcare sector.

Some **quantum sensors** have the potential to be scaled down into wearable devices [57], and improve the sensitivity of future neurotechnologies in real world situations. For example, researchers have already used advanced quantum brain imaging on drivers using virtual reality, to explore how real time brain patterns while driving change with age [58]. There are also ongoing experiments to diagnose autism and analyse brain development in young children, which is not feasible using larger existing systems [59]. Non-invasive brain **imaging** could also improve diagnosis and management of deep-brain conditions, such as Alzheimer's.

Research into **quantum machine learning** may also improve classical analysis of neurodata, and accelerate insights into brain patterns and behaviour in real world scenarios.

Beyond this, convergence of neurotechnology and quantum technologies in real world applications is still highly speculative, but could be more plausible in the longer term (15 years or more). For example, in the far future (20 years or more), it is also plausible that quantum magnetic sensors could be integrated into gaming, or even allow us to 'control' machines with thought [60]. Researchers have even speculated whether, in the far future, certain quantum imaging techniques could enable technologies that can 'read' thought [61].

Although not a common area of research, there are examples of experiments in using **hybrid and 'quantum-inspired' machine learning** approaches to improve brain computer interfaces and analysis of neurodata. For example, to improve the ways that brain computer interfaces and classical machine learning algorithms interpret and filter brain signals and images [62]. One highly speculative **quantum machine learning** example is using a future quantum computer to unlock patterns in neurodata that classical machines might not see, or help simulate the complexity of the brain [63]. It is still unclear whether this will be a suitable future use case for quantum computing.

Data protection implications

1. Processing neurodata

Such use cases are likely to involve processing neurodata, a novel and intimate type of personal information. Our neurotechnology work surfaced that neurodata is not specifically defined in UK GDPR, but the collection of information from the brain would fall within the concept of "mental identity". Additional data protection obligations apply if the neurodata is special category data (ie it reveals certain specific types of information, such as information about a person's health, ethnicity, or sexuality). Whether or not the neurodata is considered special category data is likely to depend on the use case, rather than the underlying technology used to collect it (ie the quantum sensor or specific type of neurotechnology device) [64]. Organisations using or exploring quantum technologies in a neurotechnology setting must consider their purpose for processing neurodata, and what level of protections apply. It is also always important to clarify the lawful basis for processing such information.

2. Enhanced capabilities may exacerbate wider neurotechnology risks

The sensitivity offered by quantum sensing (such as the ability to detect individual neurons firing), combined with potential advances in interpreting this information, highlights the extent of granular insight that far-future neurotechnologies could provide. As noted in our neurotechnology work, 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 (even neurodiscrimination). Other commentators have speculated and raised concerns about risks of unwarranted intrusion or even surveillance of people's thoughts and behaviours.

3. Security

Post-quantum security is also likely to be an important issue. Neurotechnologies may become more pervasive in future, in both healthcare and non-healthcare settings. Neurodata is an example of high risk information that would need to be kept confidential for a long time, particularly if being transmitted, accessed or stored for further analysis. In addition, processing neurodata may result in a high risk to people's rights and freedoms (per article 35(1) UK GDPR). It will be important to take appropriate security measures, which may include PQC, and regular deletion and appropriate retention strategies.

Next generation internet of things (IoT)

In theory, **quantum computing** could impact on the security of information transmitted by existing and next generation IoT devices, particularly those with a long lifespan such as industrial IoT, or smart buildings. In future, we could see **PQC** deployed to protect information processed by next generation smart buildings and IoT networks. However, many devices with more limited processing power may not be suitable for an upgrade.

It is unlikely that many **quantum sensing and imaging technologies** will be integrated into consumer IoT devices in the next decade. In the next 15 years, we may see pilots of IoT devices incorporating specific types of new quantum sensor or imaging technologies in public spaces, either in addition to, or instead of, current versions. This will depend on factors such as research progress and commercial interest. For example, next generation CCTV using quantum imaging that can detect the presence of (but not identify) people around corners in a hospital or park.

In 10 or more years, we may also see examples of quantum sensing and timing technologies integrated into **smart city** infrastructure, along with a range of existing sensors and imaging technologies. In particular, advanced quantum clocks could be integrated into communications infrastructure. This could help to better synchronise information flows required for real time device-to-device communication. This has the potential to help enable the ultra-fast processing required for next generation IoT systems and, even further into the future (ie 25 or more years), perhaps immersive or augmented worlds [65].

Some have speculated that next generation quantum sensing technologies could be used for functions such as:

- intrusion detection in sensitive sites;
- more precise real-time location surveillance and monitoring of traffic and transport; or
- pedestrian movement over wider areas, even in fog, traffic, or the dark.

This could enhance, for example, emergency incident response in the event of an accident or natural disaster, and future transport infrastructure planning [66].

Or, quantum sensors could be used to enhance commercial insights. For example, one type of sensor has already been piloted to detect temperature density in a shopping centre to measure shopping trends, without collecting information about identifiable people. However, in these settings, it is unclear whether emerging quantum sensors will offer a significant functional or commercial advantage compared with existing sensors.

Data protection issues

1. Security

In our first Tech horizons report, we highlighted that the security of existing and next generation IoT systems is already a key data protection issue. Depending on the use case, some of these systems can process significant volumes of personal information, which together can give insights into lifestyle and personal habits. They are susceptible to cyber attack, and many consumer IoT systems (such as smart home devices) are still working towards a ‘basic’ level of information security.

There are also specific challenges that will likely impact on the transition to post-quantum security in IoT. In particular, many IoT devices have limited processing power and need to process information quickly to function properly. It is likely that some older and less powerful devices won’t be able to use the new PQC algorithms (eg some basic environmental sensors or appliances). There are options to secure IoT at the server level, but some devices may need to be replaced entirely to secure the entire system. This could be costly and time consuming.

Some commentators suggest it is unlikely that smart home devices will be a significant priority for early transition to quantum secure systems. In the near term, we are more likely to see a transition in industrial

IoT or next generation IoT embedded in critical national infrastructure, which have a very long lifespan. We may, therefore, plausibly see a period where the next generation IoT systems most likely to process personal information that are being developed today are not protected against a future quantum computer, even if they are better adapted to current security risks. When deploying IoT, organisations and developers should ensure that they consider both current and future security updates, and adopt measures proportionate to the risks of processing.

2. Surveillance, transparency and data minimisation

Previous publications have highlighted that **next generation IoT** and **smart cities** involve high volume information collection from a wide range of sensors and cameras [67].

Adding more advanced quantum capabilities may not add any significant new risk. But, quantum technologies could feasibly pick up additional information or enable additional inferences about people's movements or use of spaces when combined with other information flows. This only falls within the scope of data protection legislation if the inferences relate to an identifiable person. Inferences about crowds, for example, rarely lead to data protection issues. Organisations can mitigate any potential impact on peoples' rights and freedoms by being clear and transparent about what they are collecting, and only collecting information that is necessary for the specific purpose (data minimisation).

Genomics

In the near to medium term future, quantum secure technologies, such as **post-quantum cryptography**, may be increasingly used by research centres, health services and private genetic testing companies to secure transfers of genomic information. QKD could also be used by some organisations to secure medical records, as has been observed in the US and Japan [68].

Researchers are also exploring how **quantum computing** and **quantum-inspired classical machine learning** could:

- help accelerate different steps in genomic sequencing and analysis (such as piecing together a genome as part of the sequencing process, or classifying sequenced genomic information) [69];
- recognise patterns in genomic sequences; and

- improve insights into interactions between multiple genes [70].

Many of these tasks are very difficult and time consuming for existing computers. Should quantum approaches fulfil their promise, it is hoped that new insights into genomic and other healthcare information could help enable personalised medicine [71].

In the UK, the National Quantum Computing Centre is also supporting a project that is exploring whether in future, hospitals could develop advanced models for genomic analysis in a privacy-preserving way, by combining **quantum computing** and **privacy enhancing techniques** [72].

Some genomics problems may turn out to be unsuitable for a quantum computer. Some approaches being tested in the genomics field are relying on (currently theoretical) quantum speedups. Major advances in genomics using quantum machine learning are also highly dependent on significant improvements in the capabilities of quantum computers and (currently speculative) quantum memory (qRAM) [73].

Data protection implications

1. Accuracy and explainability

Our Tech horizons report highlighted that accuracy is already a significant potential issue for classical genomics applications, should genomic insights be applied to people. For example, polygenic risk scores look at the potential impact of many genomic markers to estimate “an individual’s genetic risk for some trait” or disease [74]. Given the various limitations of the science, the predictive power of many polygenic risk scores vary considerably. Our report highlighted that as models improve, there is a risk that organisations (or people) overly rely on their predictive power due to a lack of understanding, or a failure to make limitations and biases clear.

A quantum computer might be used at many different stages of genomic data analysis. But, researchers are still looking into ways to verify the accuracy of outputs from a quantum computer that exceeds the capabilities of classical computers. As a result, there is a risk that using a quantum computer could introduce further potential statistical inaccuracies that are difficult to check into the genomic data analysis at different stages. This could potentially exacerbate existing concerns about the accuracy of risk scores drawing on genomic insights.

From a data protection perspective, genomics applications involve potentially high-risk inferences with significant implications for people. For example, in future, genomic insights might be used to make significant decisions about people’s health and wellbeing. It is therefore particularly important that organisations:

- clearly consider and articulate all accuracy limitations; and
- ensure inferences are not recorded as matters of fact relating to a person, but as inferences made as a result of quantum analysis.

The DRCF paper also highlighted our interest in exploring the explainability of decisions made using quantum machine learning. We may need to consider genomics use cases further, as the landscape develops. Given the state of the art, it is plausible that quantum machine learning may be used to process and analyse genomic information before the technical explainability frameworks are developed to explain the rationale behind a decision. But, equally, other types of non-technical explanation may be sufficient for organisations to fulfil their data protection obligations. Organisations should, in the first instance, refer to our existing explainability guidance.

[56] DSIT National quantum strategy (2023)

[57] Quantum Technology Hub Sensors and Timing webpage on Sensing the brain: quantum sensors; Nature Reviews Physics article: Quantum sensors for biomedical applications (2023)

[58] Quantum Technology Hub Sensors and Timing media release: New project aims to help elderly drivers keep their independence for longer (2021)

[59] University of Nottingham media release: Wearable brain imaging gives clearest ever picture of children's developing brain (2024)

[60] COMPAMED trade fair article: In focus for brain-computer interfaces: diamond-based quantum sensors

[61] University of Glasgow article: The nano and quantum world: Extreme light

[62] Cognitive Robotics article: A survey of quantum computing hybrid applications with brain-computer interface (2022); IEEE Transactions on Neural Networks and Learning Systems article on Quantum neural network-based EEG filtering for a brain-computer interface (2014); Inside Quantum Technology's "Inside Scoop:" Quantum and Neuroscience (2023); Digital Trends article: Inside the lab that connects brains to quantum computers (2023)

[63] Inside Quantum Technology's "Inside Scoop:" Quantum and Neuroscience (2023); Association for Psychological Science article: Could Quantum Computing Revolutionize Our Study of Human Cognition?

[64] ICO tech futures report on neurotechnology: Regulatory issues

[65] IEEE Conference Publication on the Application of Optical Wireless Communications in IoT Devices of Smart Grids within Smart Sustainable Cities: With Hybrid Perspectives to Metaverse & Quantum IoT; IEEE Conference publication on The Roadmap to a Quantum-Enabled Wireless Metaverse: Beyond the Classical Limits

[66] IEEE conference publication on An operator's view on opportunities and challenges of quantum internet of things (2023)

[67] See, eg, ICO First Tech Horizons Report (2022) and Berlin Group working paper on smart cities (2023)

[68] Cureus article on The Quantum-Medical Nexus: Understanding the Impact of Quantum Technologies on Healthcare (2023)

[69] Nat Methods article on Quantum computing at the frontiers of biological sciences (2021)

[70] Nature, Scientific Reports article on A biological sequence comparison algorithm using quantum computers (2023)

[71] Cureus article on The Quantum-Medical Nexus: Understanding the Impact of Quantum Technologies on Healthcare (2023)

[72] NQCC webpage on Federated quantum machine learning for genomics data

[73] Nat Methods article on Quantum computing at the frontiers of biological sciences (2021)

[74] Nuffield Department of Population Health article from the Frontiers journal on Calculating Polygenic Risk Scores (PRS) in UK Biobank: A practical guide for epidemiologists (2022)

Next steps

The transition to quantum secure systems

On the future of information security and the transition to quantum secure systems, we will:

- update our encryption guidance in line with the transition to post-quantum cryptography. We will also continue to work with NCSC and others on issues such as the ‘timeline’ for transition;
- continue to educate and raise awareness of current and future cyber risks (including the risks from a quantum computer) and available mitigations;
- continue to engage with all relevant stakeholders on the transition to postquantum cryptography. We will continue to engage with our DRCF counterparts to ensure our regulatory approaches are aligned; and
- maintain awareness of the developing landscape and standards initiatives for QKD and other quantum secure technologies to inform our understanding of the state of the art.

Organisations should:

- continue evaluating their risk exposure. This could include identifying high risk information, critical systems and at-risk cryptography;
- ensure they take evolving international standards and NCSC guidance into account, as required under NIS and UK GDPR; and
- continue adequately protecting existing information processing, including through basic cyber hygiene.

These steps are consistent with existing security obligations.

Other quantum technologies

Beyond information security questions, discussions of responsible innovation in quantum technologies are at an early stage. With the exception of some quantum sensing, timing and imaging techniques, many quantum technology use cases are more likely to mature in the medium to long term (five-15 years or more). We will need to remain alert to developing use cases and any new, emerging or exacerbated risks.

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 National Quantum Computing Centre, the UK’s quantum hubs and their pilot projects, the Office for Quantum, academia, the DRCF and other regulators; and
- explore potential applications and capabilities that may impact on people’s privacy, including use cases for:
  - **sensing, timing and imaging technologies** that could lead to an elevated risk of surveillance or other privacy harms to people;
  - **quantum computing** that could involve processing personal information or improve privacy enhancing technologies; and
  - real world pilots of **QKD**.

We encourage further discussions with organisations to ensure they embed privacy by design and default when testing and deploying quantum technologies, including during the initial pilot phase. We are also open to observing and inputting into testbeds and other regulatory sandbox initiatives for quantum technology applications that may also intersect with our remit. Initially, we will do this through DRCF and Regulators Forum, and engagement with the UK’s quantum hubs.

For any organisation developing quantum applications likely to be piloted or come to the market in the near term (in the next three years) with novel privacy implications, they can apply to our sandbox. However, based on current timescales, we anticipate such applications for technologies such as quantum sensing and timing in a few years time, and for quantum computing in the longer term.

This report reflects our early-stage thinking. We welcome contact from any stakeholders wishing to continue the conversation. We encourage organisations exploring applications that may involve processing personal information, or novel uses of quantum technologies and privacy enhancing technologies, to contact us at: [email protected].

Annex: Glossary

Superposition and **entanglement**:

Two different features of particles behaviour at the atomic and subatomic level that quantum technologies use to unlock new capabilities.

A spinning coin is, in a way, both heads and tails until it falls one way or another. Similarly, according to quantum mechanics, atoms, electrons and particles of light (photons) can be in two (or more) states at once, until they are measured. This state is known as **superposition**. In quantum computing, for example, a qubit (a unit of quantum information) can be a combination of both a zero and one at the same time, until it is measured. QKD also uses this property to securely share an encryption key. When the key is sent in a quantum state, any attempt to copy, intercept or eavesdrop would introduce detectable errors.

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 how far away they are from each other [75]. 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 line of sight.

Chapter one

Quantum magnetic sensors: These exploit quantum properties to detect tiny changes in magnetic fields.

Quantum gravity sensors: Rather than using radio frequencies like conventional radar, a certain class of these sensors use falling clouds of cold atoms in two states (superposition) to detect tiny changes in the Earth’s gravitational field caused by objects [76].

Optical clocks: Current atomic clocks (eg those used on GPS satellites) measure the frequency of microwaves needed to change how electrons move around the nucleus of atoms. This gives a highly precise measurement of time [77]. Developments in optical clocks, a new version of an atomic clock, use lasers instead of microwaves, which give the possibility of even more precise measurements [78].

Quantum key distribution: This is a way of securely sharing encryption keys using quantum phenomena. The key is sent as a quantum light pulse, which changes when measured. So, any attempt to copy, intercept or eavesdrop when sending the encryption key would introduce detectable errors [79].

Fully homomorphic encryption: This is one of three types of homomorphic encryption. Homomorphic encryption allows you to perform computations on encrypted information without first decrypting it. Fully homomorphic encryption has no limitations in terms of the types of operations it supports or their complexity. However, the more complex the operation, the more resource and time may be required [80].

Chapter four

Quantum random number generation: This technique involves using the principles of quantum physics to generate “truly random” numbers for classical encryption keys. It is one of several techniques designed to be more resistant against the capabilities of a future quantum computer.

Hybrid cryptography schemes: These combine classical and post-quantum cryptography approaches.

Cryptographically relevant quantum computer: A quantum computer that can efficiently solve the mathematical problems that underpin existing public key cryptography. Expert timescale estimates vary for when such a computer will emerge, if it ever does.

Encryption: "Information is encrypted and decrypted using a secret key. (Some algorithms use a different key for encryption and decryption)… In practical terms it will take such a long time to find the right key—ie many millions of years, depending on the computing power available and the type of key—that it becomes effectively impossible" [81].

Asymmetric cryptography (such as Rivest–Shamir–Adleman, or RSA encryption): "Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key. The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large. Data encrypted with the recipient's public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data." [82]

Asymmetric cryptography has two common functions:

- to securely share cryptographic keys before encrypting a message, including before encrypting a message using **symmetric cryptography** (**key agreement**); and
- for **digital signatures**, a way of authenticating or proving who someone or a device is before they enter into a transaction, share keys, join a network or download a security update [83].

Symmetric cryptography: "In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient." [84] It currently common practice for the sender to share the key using asymmetric cryptography to ensure the key remains secret/confidential. A quantum computer would be able to break the encryption protecting the secret key, and therefore use the key to decrypt the secure transmission. According to NIST, this puts the information these keys protect (including communications and stored information) at risk of exposure or "undetected modification" [85].

Digital signatures: These are commonly used to establish that an "entity" (such as a computer, mobile or IoT device) seeking access to an online network or to exchange cryptographic keys is who they claim to be, and should be allowed access to the network. They are also commonly used to authenticate financial transactions and "can provide a level of trust that an email has not been intercepted or spoofed" [86].

Zero knowledge proof: This is a privacy enhancing technology. It involves using a set of instructions to prove information without disclosing it. For example, a person could prove their age or whether they are financially solvent, without needing to disclose that information [87].

[75] NQCC webpage on Quantum features

[76] UK National Quantum technologies programme article: Gravity sensors see underground (2021)

[77] NASA article: What is an atomic clock?

[78] University of Birmingham media release: Next generation atomic clocks are a step closer to real world applications (2022)

[79] Quantum Communications Hub article on QKD

[80] ICO PETs guidance: Homomorphic encryption

[81] ICO encryption guidance: What is encryption?

[82] ICO guidance on encryption: What types of encryption are there?

[83] NCSC whitepaper on preparing for quantum-safe cryptography (2020)

[84] ICO guidance on encryption: What types of encryption are there?

[85] NIST cybersecurity white paper on getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms (2021)

[86] ICO guidance on encryption: Encryption scenarios

[87] ICO PETs guidance: Zero-knowledge proofs

Annex: Acknowledgements

With special thanks to the following for their contribution to our research:

- Dr Sonali Mohapatra and Dr Natasha Oughton, National Quantum Computing Centre, UK
- Dr Keith Norman, UK Quantum Computing and Simulation Hub
- Professor Timothy P. Spiller, UK Quantum Communications Hub
- Dr Ross Grassie and Dr Petros Wallden, UK Quantum Software Lab
- Bengi Zeybek, Law and Governance of Quantum Technologies Research Group, University of Amsterdam
- Dr Juljan Krause, University of California Institute on Global Conflict and Cooperation
- Professor Martin Albrecht, Dr Ngoc Khanh Nguyen, Dr Eamonn Postlethwaite, King’s College London
- Professor Rem Noormohamed, Fieldfisher LLP