Guidance on consumer Internet of Things products and services: Impact Assessment - DRAFT

ico.
Information Commissioner's Office

Contents

Executive summary

This draft impact assessment accompanies our draft guidance on consumer Internet of Things (IoT) products and services. It sets out **our initial impact considerations for consultation**, alongside the consultation on the draft guidance. It should be noted that this is not an exhaustive assessment of the impacts of the guidance, and we will move towards a more conclusive assessment of impact based on the development of the final guidance and taking account of the feedback received at consultation stage. We are **seeking feedback on this draft impact assessment, along with any additional information or insights that stakeholders may be able to provide on impacts** throughout the consultation process.

Problem definition

The draft guidance covers the processing of personal information by organisations providing IoT products on the consumer market. Much of the data processing in IoT products relates to tracking user activity. The ICO's Online Tracking Strategy identifies areas where people are not being given the control they are entitled to under data protection law. These areas are present across a wide range of websites, services and technologies (including IoT devices), affecting nearly all adults online. **When users lack control, harm can occur. It is recognised that there are particular problems for IoT products and services in complying with data protection legislation, for instance in the delivery of privacy information.** ICO intervention is required to **provide clarity on our regulatory expectations** to organisations who process personal information in consumer IoT products.

Rationale for intervention

The combination of compliance concerns, data protection harms and market failures have **prompted the ICO to determine that action needs to be taken to improve regulatory certainty on how PECR and GDRP regulations apply to IoT products and services**. Absent regulatory intervention, firms are likely to continue to underinvest in data protection, consumers are likely to be exposed to increasing data protection risks over time and wider society is likely to face increased costs of harm mitigation.

Options appraisal

In the context of the identified problem and rational for intervention, six options were considered. These options were assessed against a number of critical success factors and the preferred option of **light touch engagement plus guidance (Option 5)** was chosen. This option involves the provision of a light

touch regulatory approach using education, engagement and influence alongside the development of support and guidance setting out ICO expectations across the wider IoT market.

Details of proposed intervention

The proposed regulatory intervention involves light touch engagement plus guidance. The overarching objective of the guidance involves the provision of **regulatory certainty** to organisations. The production of guidance for consumer IoT products and services, aims to help organisations provide people with meaningful control across the AdTech ecosystem; reduce the potential for data protection harms; and meet the objectives noted. These include: a level playing field of compliance amongst organisations is achieved; innovative alternatives are developed and implemented; and organisations respect and adhere to people's choice to name a few.

Cost-benefit analysis

Our initial analysis of costs and benefits has identified a number of impacts of the draft guidance including the reduced potential for data protection harms. The guidance is expected to increase regulatory certainty for organisations within the consumer IoT ecosystem. Although there will be costs to organisations from reading, understanding and implementing the guidance, this is expected to be outweighed by the wider societal benefits of reduced data protection harms.

At this initial draft stage of guidance development, we **expect the guidance to have a net positive impact on balance**. However, we will seek to gather additional information on the potential costs and benefits of the guidance throughout consultation and development of our final guidance and impact assessment.

Monitoring and evaluation

As per our impact assessment framework, when finalising the guidance post consultation, we will consider the monitoring and review processes. As noted, this intervention sits within our wider Online Tracking Strategy. As such, the outcomes and impacts of this intervention will feed into any wider ex-post impact measurement carried out on the Online Tracking Strategy.

1. Introduction

This document sets out a draft impact assessment of our proposed intervention, to **provide regulatory certainty among organisations who process personal information in consumer Internet of Things (IoT) products and services**. The guidance explains how data protection law including UK General Data Protection Regulation (UKGDPR),[1] and the Privacy and Electronic Communications Regulations 2003 (PECR)[2] apply when you process personal information in consumer IoT products and services.

The intervention involves the provision of **light-touch engagement plus guidance on consumer IoT products and services**; and sits within our wider Online Tracking Strategy.[3] This strategy sets out the ICO's commitment to 'giving people meaningful control over how they are tracked online, enabling them to go about their online daily lives with trust and confidence'.

The intervention for consumer IoT products and services aims to enable organisations to comply with data protection legislation. This includes objectives to help organisations to design in privacy from the get-go (or retro-fit it where appropriate); to limit the use and sharing of people's information to the appropriate purposes; and to reduce the potential for data protection harms.

1.1. Our approach to the impact assessment

The purpose of impact assessment is to improve regulatory interventions and policy-making by:

- informing decision-makers about potential economic, social, and (where relevant) environmental ramifications;
- providing a mechanism to consider the impact of interventions on a range of stakeholders, including different groups of citizens and organisations;
- improving the transparency of regulation by explicitly setting out the intervention theory of change and the quality of underlying evidence;
- increasing public participation in order to reflect a range of considerations, improving the legitimacy of policies;
- clarifying how public policy helps achieve its goals and priorities through policy indicators; and

[1] UK Government (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Available at: https://www.legislation.gov.uk/eur/2016/679/contents (accessed 31 May 2025).
[2] UK Government (2003) *The Privacy and Electronic Communications (EC Directive) Regulations 2003*. Available at: https://www.legislation.gov.uk/uksi/2003/2426 (accessed 31 May 2025).
[3] ICO (2025) *Our strategy for levelling the playing field for online tracking in 2025.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/01/our-strategy-for-levelling-the-playing-field-for-online-tracking-in-2025/ (accessed 31 May 2025).

- contributing to continuous learning in policy development by identifying causalities that inform ex-post review of interventions and improve future policy-making.

This document **sets out our initial impact findings alongside the publication of draft guidance**. It is important to note that this isn't an exhaustive assessment; we will develop our analysis further as we move towards publication of the final guidance, based on any additional information and feedback received. We are **seeking feedback on this draft impact assessment, as well as any other information and insights stakeholders can provide on impacts through the consultation process**.

We have assessed the potential impacts of the proposed guidance on consumer IoT products and services using cost-benefit analysis, which aims to identify the full range of impacts by assessing both the costs and benefits of the guidance. Our approach follows the principles set out in the ICO's Impact Assessment Framework,[4] which in turn is aligned with HM Treasury's Green Book,[5] Regulatory Policy Committee guidance,[6] and Business Impact Target guidance on best practice for impact assessments.[7]

In identifying the potential impacts of the guidance, it is important to distinguish between:

- Impacts that can be attributed to the guidance. These are affected by how the ICO chooses to develop the guidance.
- Impacts that are not attributable to the guidance. These are impacts that simply arise from the existing legislative requirements that controllers are already expected to comply with.

For the purposes of the impact assessment, we are interested in impacts that are attributable to the guidance, rather than those that arise from existing legislative requirements.

---

[4] ICO (2023) *The ICO's Impact Assessment Framework*. Available at: https://ico.org.uk/media/about-the-ico/documents/4027020/ico-impact-assessment-framework.pdf (accessed 31 May 2025).
[5] HMT (2020) *The green book*. Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020 (accessed 31 May 2025).
[6] BEIS (2020) *Better Regulation Framework – Interim Guidance*. Available at: https://regulation.org.uk/library/2020-Better_Regulation_Framework-interim_guidance.pdf#:~:text=This%20interim%20guidance%20explains%20how%20the%20better%20regulation,replaces%20the%20Better%20Regulation%20Framework%20Guidance%20August%202018 (accessed 31 May 2025).
[7] BEIS (2017) *Business Impact Target: Appraisal of guidance: assessments for regulator-issued guidance*. Available at: https://assets.publishing.service.gov.uk/media/5a8234fbe5274a2e8ab580e8/business-impact-target-guidance-appraisal.pdf (accessed 31 May 2025).

1.2. Report structure

The structure of this report is as follows:

- **Section 2 - Problem definition:** sets out the evidence base to support the identification of the problem that the intervention aims to address.
- **Section 3 - Rationale for intervention:** considers the rationale for intervention by exploring whether there is market failure and highlighting the economic, social and political context.
- **Section 4 - Options appraisal:** provides a review of policy options against the critical success factors of the intervention.
- **Section 5 - Details of proposed intervention:** provides an overview of the proposed guidance and sets out the key groups we expect to be impacted by our intervention.
- **Section 6 - Cost-benefit analysis:** presents and analyses the identified costs and benefits of the guidance, across each of the affected groups identified.
- **Section 7 - Monitoring and evaluation:** outlines future monitoring considerations to ensure the impact of the intervention and any lessons learned are captured.
- **Annex A: -** provides more detail on how familiarisation costs are estimated to support the assessment of costs and benefits.

2. Problem definition

In this section we define IoT and consumer IoT products and services. We then set out the problem that our intervention aims to address. This includes providing a baseline of the current situation comprising of an overview of available research and evidence to estimate the size of the consumer IoT products and services market. We also identify some of the issues noted within this market in relation to privacy and data protection.

2.1. What is the consumer Internet of Things?

According to the Government Office for Science (Go-Science);[8] in its most basic form, the IoT connects 'smart' devices through the internet to collect and share data. IoT is a broad term applied to devices incorporating internet connectivity, ranging widely from smart watches and locks to connected vehicles.

IoT products and services can process large amounts of often highly personal data about people who use them and people who are exposed to them. The devices typically incorporate multiple technologies; for example, biometric and environmental sensors, artificial intelligence and machine learning, encryption, and cloud computing; and enable processing of personal data at scale.

The Organisation for Economic Co-operation and Development (OECD)[9] divides IoT products and services into the following categories:

- **Consumer IoT** which includes a variety of devices, such as health monitors and smart home applications.
- **Commercial IoT** which concerns applications developed to provide a better experience to people in places like hotels and restaurants, through elements such as connected lighting or building access in smart buildings and smart offices.
- **Enterprise IoT** which includes diverse technologies to enable new business applications, that connect with physical objects and enterprise systems (enterprise resource planning and customer relationship management).
- **Industrial IoT** which includes devices that can be implemented across multiple sectors, including agriculture and healthcare, as well as government and cities.

[8] Government Office for Science (2021) *Trend Deck 2021: Technology.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/993981/GO-Science_Trend_Deck_-_Technology_section_-_Spring_2021.pdf (accessed 31 May 2025).
[9] OECD (2021) *Measuring the Internet of Things.* Available at: https://www.oecd.org/en/publications/measuring-the-internet-of-things_021333b7-en.html (accessed 31 May 2025).

The draft guidance covers the processing of personal information by organisations providing IoT products on the consumer market. Some further examples of **consumer IoT** products include:

- home entertainment products (smart speakers, connected TVs, connected toys);
- home automation products (smart lights and lightbulbs, smart thermostats, smart home hubs);
- domestic appliances (smart fridges, smart ovens);
- wellbeing products (fitness trackers, smart watches, smart scales, sleep monitors);
- security and safety products (smart security cameras, smart doorbells, smart baby monitors);
- over-the-counter medical devices (smart fertility trackers with a device, smart blood pressure monitors, smart pulse oximeters); and
- peripheral products (smart keyboards, smart mice, smart headphones).

2.2. Problem context

As stated in the Department for Science, Innovation and Technology (DSIT) 2018 Code of Practice for consumer IoT security: 'People should be able to benefit from connected technologies safely, confident that adequate security and privacy measures are in place to protect their online activity'.[10] The consumer IoT market is recognised to hold many potential benefits for both people and organisations.[11] However, it is also noted that consumer IoT products and services can present numerous privacy and security risks to those that interact with them.[12]

Recent ICO funded research noted that 'in the consumer IoT, different types of data are collected and shared in various ways, yet the specifics of such often remain opaque. Furthermore, what happens to data after it is sent to others is unclear – despite the use of data transparency rights. This is concerning, given the personal and intimate domestic settings in which consumer IoT devices operate'.[13] For example, wearable devices may collect personal information such

[10] UK government (2018) *Code of Practice for consumer IoT security*. Available at: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security (accessed 31 May 2025).
[11] Corbett (2013) *Using information systems to improve energy efficiency: Do smart meters make a difference?* Available at: https://link.springer.com/article/10.1007/s10796-013-9414-0 (accessed 31 May 2025).
[12] DSIT (2023) *A Review on the Risks and Psychological Harms Presented by Consumer IoT Products*. Available at: https://assets.publishing.service.gov.uk/media/672b676dfbd69e1861921c21/A_review_of_the_risks_and_psychological_harms_presented_by_consumer_IoT_products_-_Cote_et_al.pdf (accessed 31 May 2025).
[13] University of Cambridge and Imperial College London (2023) *Transparency in the consumer Internet of Things.* Available at http://www.iot-transparency.org/ (accessed 31 May 2025).

as date of birth or email address; data on people's behaviours, location or interactions with the product; or special category data such as biometric data or health metrics. The research noted that 'currently, there is limited visibility over the nature of data processing that occurs in the consumer IoT'; and 'many IoT products transmit data to a range of locations, though the reasons and rationales for such transmissions can be unclear'. There are also numerous wider reports of misuse of data gathered through IoT devices; such as a lack of security measures leading to smart doorbell systems being hacked;[14] and indefinite data retention periods for children's voice data from smart speakers along with inability of the parents to delete it.[15]

These issues are increasingly important because the consumer IoT market has grown significantly over recent years,[16] and in 2023 Tech UK estimated that the percentage of UK adults that owned at least one smart (or 'connected') home device (including wearables) was around 80%; with adoption trends predicted to continue rising.[17]

At the same time, it is recognised that there are particular challenges for IoT products and services in complying with data protection legislation, for instance in the delivery of privacy information. As recognised within ICO guidance on the UK GDPR right to be informed,[18] IoT devices such as home assistants, connected toys and smart meters often don't have screens on which to provide individuals with written information about the use of their data.

2.3. Consumer IoT market within the UK

In order to inform our understanding of the use of consumer IoT products and services in the UK, we have carried out desk research looking at both the supply side (manufacturing and wider supply-chain of IoT products and services) and demand side (consumer interaction with IoT devices).

---

[14] FTC (2023) *FTC Says Ring Employees Illegally Surveilled Customers*. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users (accessed 31 May 2025).
[15] FTC (2023) *Out of the mouths of babes?* Available at: https://www.ftc.gov/business-guidance/blog/2023/05/out-mouths-babes-ftc-says-amazon-kept-kids-alexa-voice-data-forever-even-after-parents-ordered (accessed 31 May 2025).
[16] Corbett (2013) *Using information systems to improve energy efficiency: Do smart meters make a difference?* Available at: https://link.springer.com/article/10.1007/s10796-013-9414-0 (accessed 31 May 2025).
[17] TechUK (2023) *State of the connected home 2023.* Available at: https://www.techuk.org/resource/state-of-the-connected-home-2023.html (accessed 31 May 2025).
[18] ICO (2025) *What methods can we use to provide privacy information*? Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/#how7 (accessed 31 May 2025).

Due to the broad range of industries involved within the consumer IoT market, its difficult to provide estimates of market size, and in turn, the consumers that interact with the market. However, in the following sections we provide an overview of available evidence on the approximate size and scale of demand and supply within the consumer IoT market.

2.3.1. Demand side

The level of consumer interaction with IoT products and services is significant within the UK market. In 2020 Ofcom[19] research illustrated that around a third of adults had at least one internet-connected device in their household. Whilst according to TechUK,[20] by 2023 around 80% of UK adults owned at least one device, with adoption trends predicted to continue rising. Tech UK's research also noted significant growth in the number of 'advanced adopters' (defined as people that own more than three connected home devices); from 26% in 2022, to 34% in 2023.

TechUK asked consumers to project how much they think they will spend on smart and connected home devices over the coming 12 months. The estimates suggested that around 25% of consumers expected to spend more than the previous year on smart devices, with this figure increasing to 40% among 'advanced adopters'. Only 18% of consumers expected to spend less on smart home devices in the following year.

Given the evidence outlined, we could assume that approximately 80% of the UK population (aged 16+) could be currently considered users of IoT products and services. This equates to approximately 45 million people.[21]

As noted by the United States Federal Trade Commission (FTC),[22] due to the presence of IoT products such as smart speaker devices in consumers' homes, along with the sale of child-centric smart speaker products, there are also many users of these technologies aged under 13. These devices, along with smart

[19] Ofcom (2020) *Online Nation Report*. Available at: https://www.ofcom.org.uk/data/assets/pdf_file/0027/196407/online-nation-2020-report.pdf (accessed 31 May 2025).
[20] TechUK (2023) *State of the connected home 2023.* Available at: https://www.techuk.org/resource/state-of-the-connected-home-2023.html (accessed 31 May 2025).
[21] ONS (2024) *UK population mid-year estimate 2022*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates (accessed 31 May 2025).
[22] FTC (2023) *Out of the mouths of babes? FTC says Amazon kept kids' Alexa voice data forever – even after parents ordered deletion*. Available at: https://www.ftc.gov/business-guidance/blog/2023/05/out-mouths-babes-ftc-says-amazon-kept-kids-alexa-voice-data-forever-even-after-parents-ordered (accessed 31 May 2025).

doorbells and smart security cameras have the potential to gather data on those outside of the consumer's home also, such as visitors.

Given the evidence outlined, we could assume that the entire UK population could be currently considered within the wider population of those potentially interacting with IoT products and services. This equates to approximately 68 million people.[21]

Issues and barriers to demand for consumer IoT products

In February 2024 the ICO published the findings from a Citizens' Jury which was held over two online workshops, with 22 participants. The workshops were held to gather evidence on people's experience with IoT products and common challenges related to their privacy and security, in order to inform policy considerations on consumer IoT.[23] The report stated that participants:

- grew more concerned about privacy and security of IoT over the course of the workshops;
- discussed how privacy and security measures could be introduced throughout the lifecycle of IoT products;
- are unclear about privacy and security features before purchasing.
- find it hard to engage with privacy information and consent choices during setup and make choices on behalf of others;
- didn't tend to think about privacy after setting up IoT products, but they did voice concerns about data sharing with other household members; and
- generally, don't consider privacy when disposing of IoT products and are sceptical when they do try to delete information

The TechUK survey also asked consumers what they thought were the main barriers to owning smart home products. After concerns around costs, concerns around personal privacy were noted as the next most significant barrier across each product category (Smart Domestic Appliances, Smart Entertainment, Smart Energy & Lighting, Smart Health Monitors and Smart Security & Control), as illustrated in Table 1.

[23] ICO (2023) *IoT Citizen Jury Report*. Available at: https://ico.org.uk/media2/migrated/4029712/iot-citizen-jury-report.pdf (accessed 31 May 2025)

Table 1: Barriers to owning smart home products

Smart products	I would be concerned about personal privacy	I am concerned about this technology and the impact on security in my home
Smart Domestic Appliances	52%	39%
Smart Entertainment	51%	36%
Smart Energy & Lighting	44%	40%
Smart Health Monitors	52%	40%
Smart Security & Control	49%	33%
Overall	50%	38%

Source: ICO Analysis, Tech UK.[20]

Privacy concerns were cited as an issue by 50% of consumers overall, while the highest proportions of those reporting concerns around privacy were within domestic appliances, smart security and control, and smart entertainment categories. Respondents to the TechUK survey were also concerned about the impact of IoT technologies on security in their home in general.

However, according to some industry reports,[24] while the details around what an IoT product or service will do with your data may be outlined within the privacy policy or Terms and Conditions; around a third of those surveyed by Which?, admitted to not reading any of the privacy policy when downloading the app, while two thirds said that they merely skimmed it'.

According to the FTC there are issues with misrepresentation and compliance by devices such as smart speakers.[25] While this data relates to the US market, we are aware that many of these devices are also bought by UK consumers. The FTC asserted that Amazon had saved both adult's and children's voice recordings as audio and text files and used persistent identifiers to connect those files to Amazon profile data. As noted in the previous section, children may interact directly with devices such as smart speakers and may use an individual profile, which links to their parent's profile and contains the child's name, birth date, and gender.

According to TechUK another key consideration in the market for connected home devices is the ability of devices to connect and interact with other smart devices within the home, with 80% of consumers indicating that this was

[24] Which? (2023) *The smart device brands harvesting your data*. Available at: https://www.which.co.uk/news/article/the-smart-device-brands-harvesting-your-data-al4vp6Z3ePDf (accessed 31 May 2025).
[25] FTC (2023) *Out of the mouths of babes? FTC says Amazon kept kids' Alexa voice data forever – even after parents ordered deletion*. Available at: https://www.ftc.gov/business-guidance/blog/2023/05/out-mouths-babes-ftc-says-amazon-kept-kids-alexa-voice-data-forever-even-after-parents-ordered (accessed 31 May 2025).

'essential or quite important when considering a new smart product for the home'. This proportion rose to 96% among advanced adopters.

Concerns around privacy are noted by around 50% consumers to be a significant barrier to owning smart home products. However, around a third of consumers survey by Which?, admitted to not reading a privacy policy when downloading an app, with two thirds merely skimming the detail.

Personal safety was also noted by consumers as a concern, while interaction across devices is important to a high proportion (at least 80%) of consumers.[20]

Due to the presence of IoT devices in and around the home, there is potential for interaction with others within the consumer's household, such as those under 13 years of age.

2.3.2. Supply side

In order to measure the size of the consumer IoT market, we need to have a clear definition of that market. However, as we note at the beginning of Section 2.1, there is no universally accepted definition of IoT; nor is it possible to isolate those organisations and businesses that operate within the market (for instance, by using Standard Industry Classification (SIC) codes).[26]

While the data presented in this section gives an overview of the sector, the limitations of this analysis mean that it is difficult to compare metrics or interogate the data to ensure it doesn't include elements that are outside the scope of this guidance (such as industrial IoT devices). As a result we have adopted a range of metrics to provide a baseline understaning of the sector/market and illustrate some of the potential future trends, using proxies where possible to give a sense of the supply side behaviours.

Value of the 'Consumer IoT' market in the UK

There are a number of market reports that attempt to place an approximate value on the current and future consumer IoT sector globally; however, estimates on the value of this market in the UK are less readily available. Table 2 gives an overview from two reports that provide an estimated value of consumer IoT in the UK market specifically. The reports provide an estimated value of between $4 billion and $5 billion, which equates to approximately £3 billion to £4 billion (around 0.4%-0.5% of UK GDP); with projections of between $7 billion and $9 billion (approximately £5 billion to £7 billion) by the year 2032.

[26] ONS (2007) *UK Standard Industrial Classification of Economic Activities*. Available at: https://www.ons.gov.uk/methodology/classificationsandstandards/ukstandardindustrialclassificationofeconomicactivities (accessed 31 May 2025).

Table 2: Selected estimates of current and future value of the UK market for consumer Internet of Things (IoT)

	Estimated UK market value: approximate value in GBP (£ billions)[27]	
Source	**2024**	**2030**
Grand View Research[28]	£2.8	£6.7
Statista[29]	£3.6	£5.3

Source: ICO analysis.

TechUK also tried to assess the overall value of the UK connected home sector through points of sales tracking data,[30] with estimates for the period 2022-2023 of £4.9 billion. The report illustrated an overall decline in sales volume since 2020/21 at around 2% year-on-year and a similar fall in sales value by around 3% from £5.1 billion in 2021/22.

Types and origins of 'consumer IoT' products sold in the UK

In 2024, DSIT published a study, which aimed (among other things) to map and analyse the market for consumer connectable products.[31] The study used a combination of desk research, along with field surveys to collect primary data across 33 manufacturers. The study noted a range of IoT products being sold within the UK, as illustrated in Table 3.

Table 3: Consumer connectable products sold in the UK, by category

Product type	Proportion of products sold
Safety & Security	22%
Lighting	11%
Smart Home	10%
Kitchen appliances	7%

[27] Approximate GBP (£) values provided at rate 1 USD ($) = 0.742488 GBP (£)
[28] Grandview. Available at: https://www.grandviewresearch.com/horizon/outlook/iot-devicesmarket/uk#:~:text=The%20UK%20iot%20devices%20market%20generated%20a%20revenue,was%20the%20largest%20revenue%20generating%20component%20in%202024. (accessed 31 May 2025)
[29] Market Insights Statista. Available at: https://www.statista.com/outlook/tmo/internet-of-things/consumer-iot/united-kingdom (accessed 31 May 2025)
[30] Tech UK (2023) *State of the Connected Home*. Available at: https://www.techuk.org/resource/state-of-the-connected-home-2023) (accessed 31 May 2025).
[31] DSIT (2024) *Cyber security of consumer IoT - manufacturer survey*. Available at: https://www.gov.uk/government/publications/cyber-security-of-consumer-iot-manufacturer-survey/cyber-security-of-consumer-iot-manufacturer-survey (accessed 31 May 2025)

Audio	7%
Health, Fitness & Wellbeing	6%
Wearables	6%
Environmental Control	6%
Home appliances	4%
Other	21%

Source: ICO analysis, DSIT (n=1,024 products).[31]

The research found that safety and security products were the most popular product sold within the UK, while smart home, lighting and kitchen appliances made up an additional 28% of product sales. Further analysis by TechUK,[32] found that a very high proportion of new televisions are 'smart', and this sector remains the largest driver of value in the smart home market.

The market research carried out by DSIT found that the products sold within the UK market were made by manufacturers headquartered in 28 countries. However, as shown in Figure 2, around 78% of the products came from manufacturers in just five countries: the USA, China, the UK, Germany, and Japan, with the UK market estimated to supply around 14% of the products surveyed.

Table 4: Consumer connectable products sold in the UK, by country of origin

Country	Proportion of products sold
USA	28%
China	25%
UK	14%
Germany	7%
Japan	4%
Other	23%

Source: ICO analysis, DSIT (n=1,024 products).[31]

Size and scale of the UK 'consumer IoT' market

It is not possible to isolate those organisations and businesses that operate within the UK consumer IoT market (for instance, by using SIC codes).[33]

[32] Tech UK (2023) *State of the Connected Home*. Available at: https://www.techuk.org/resource/state-of-the-connected-home-2023) (accessed 31 May 2025).
[33] ONS (2007) *UK Standard Industrial Classification of Economic Activities*. Available at: https://www.ons.gov.uk/methodology/classificationsandstandards/ukstandardindustrialclassificationofeconomicactivities (accessed 31 May 2025).

However, the ICO Data Controller Study (DCS),[34] asked over 2,000 organisations whether they provide an online or internet enabled service and if so, which services they provide. Of those organisations that responded, 13% stated that they provide 'electronic services controlling connected toys and other connected devices'.

The OECD report on Measuring the Internet of Things,[35] provides further estimates drawing on data from Crunchbase (a commercial database on innovative companies).[36] The database classified 10,384 international firms as active in the IoT sector, as of May 2021. However, the report notes that as 'IoT is a technology diffused to several sectors, complementary to other technologies and enabling diverse applications and use', some firms may have been left out of this classification. A further search based on a list of keywords drawn from IoT-related patents (noted within the report as including 'IoT', 'smart device', 'home automation' and others), identified an additional 2,913 IoT firms, bringing the total estimated number of IoT firms to 13,296.

A 2023 OECD report,[35] notes the difficulties in adequately measuring the number of IoT firms; estimating that around 13,000 innovative firms were operating in the global IoT market in 2021.

Size of organisations within the 'consumer IoT' market

Results from a DSIT report into the market for consumer connectable products,[37] show that the market is characterised by large players. As indicated in Table 5, around 37% of the 394 organisations analysed were large organisations with more than 250 employees, while 49% were considered to be Small to Medium Enterprises (SMEs) with less than 249 employees, and just 8% were micro-organisations with fewer than ten employees. Turnover data also reflected this trend with 29% of the manufacturers surveyed having a turnover of over £50 million.

[34] ICO (2024) *Data Controller Study*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/data-controller-study/ (accessed 31 May 2025).
[35] OECD (2023) *Measuring the Internet of Things*. Available at: https://www.oecd.org/en/publications/measuring-the-internet-of-things_021333b7-en.html (accessed 31 May 2025).
[36] Crunchbase is a commercial database on innovative companies started in 2007. Available at: www.crunchbase.com (accessed 31 May 2025).
[37] DSIT (2024) *Cyber security of consumer IoT - manufacturer survey*. Available at: https://www.gov.uk/government/publications/cyber-security-of-consumer-iot-manufacturer-survey/cyber-security-of-consumer-iot-manufacturer-survey (accessed 31 May 2025).

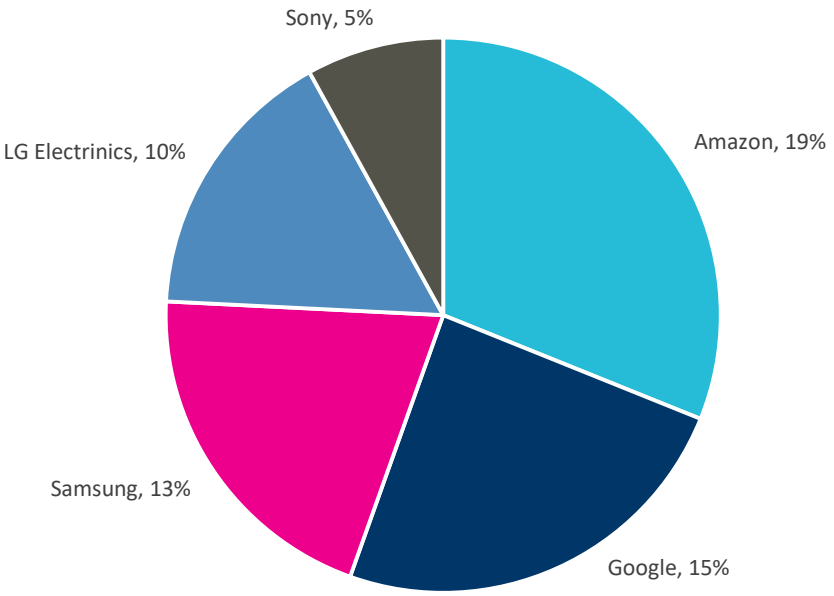
Table 5: Manufacturers of consumer connectable products, by size

Organisation size	Proportion of manufacturers
Large: 250+ employees	37%
Medium: 50-249 employees	21%
Small 10-49 employees	20%
Micro: 1-9 employees	8%
Data unavailable[38]	14%

Source: ICO analysis, DSIT (n=394 products).

Analysis by the Internation Data Corporation (IDC) in 2020,[39] set out the top five smart home device vendors within Europe at that time. Amazon was noted to hold the largest proportion of the vendor shipment market with 19% of the market share, while Google held the second largest market share at 15% as noted in Figure 1.

Figure 1: Distribution of the European market in the last quarter of 2019



Source: ICO analysis, IDC quarterly smart home device tracker.[39]

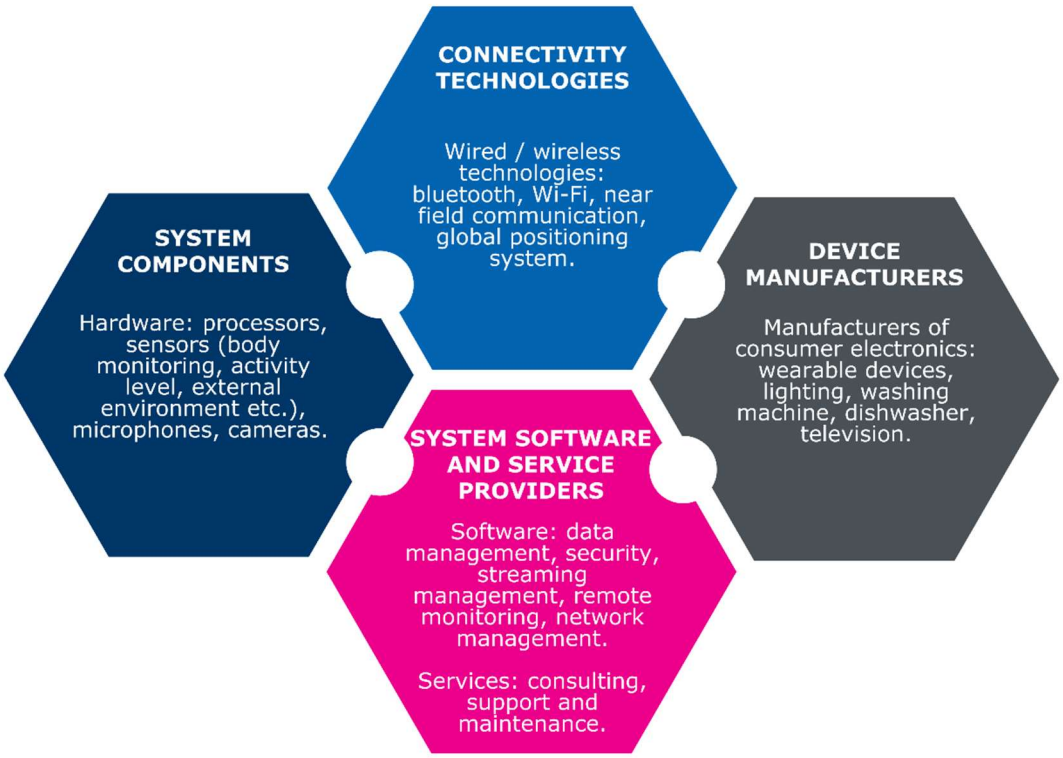
Device vendors make up just a small section of the overall supply chain within the IoT market. It is also recognised that while large IoT manufacturers may produce multiple products and incorporate multiple capabilities such as in-house

[38] According to the report 'It was not possible to find information on the number of employees for the remaining 14% of companies'.
[39] IDC (2021) *Worldwide Quarterly Smart Home Device Tracker*. Available at: https://techmindvc.substack.com/p/smart-home-notre-nouveau-rapport (accessed 31 May 2025).

software and hardware manufacture; this is unlikely to be the case for smaller manufacturers who may concentrate on one element or a small section of the wider consumer IoT product and service ecosystem.

The following Figure 2 illustrates the wide range of system components, system software and service providerss, device manufactureres, and connectivity technologies involved within the consumer IoT ecosystem.

Figure 2: Consumer IoT ecosystem



Source: ICO analysis.

The IoT market is characterised by large players,[37] with approximately 37% considered to be large organisations.

A complex ecosystem exists incorporating system components, system software and service providerss, device manufactureres, and connectivity technologies. Larger organisations may have many of these capabilities in-house, while this is unlikely to be the case for SMEs.

Wider supply chain

Measuring the numbers of organisations involved in the wider supply chain of consumer IoT products and services is difficult given the data and evidence currently available to us.

While we know that organisations use information on how people use their online products and services to inform service improvements, we also know that this information can be used to track individuals with a view to providing online advertising, alongside other non 'strictly necessary' use cases. Given that IoT products and services process large amounts of often highly personal data about people who use them and people who are exposed to them, there is the potential for significant interaction between the use of IoT products and services and the online advertising sector as a whole. According to some industry reports, 'smart TV menus are now flooded with adverts, some of them personalised based on your data'.[40]

As outlined within our draft impact assessment on the use of storage and access technologies,[41] the online advertising market is based on the sale of advertising space by online service providers to other organisations wishing to target consumers of that online service. According to industry research around 81% of SMEs that use paid-for online advertising say it is important to their business success, with 64% of UK SMEs (roughly 3.5 million organisations) having used some form of paid online advertising in the last year.[42]

According to UK business statistics there are approximately 5.5 million businesses across all sectors within the UK, with around 3.5 million of those considered to be SMEs that have used some form of paid online advertising in the last year.[43]

Issues within the 'consumer IoT' market

Research by the consumer organisation Which?,[44] has noted 'excessive smart device surveillance' across a range of device types. While academics at the University College London[45] tested two major smart TV brands (LG and

[40] Which? (2023) *The smart device brands harvesting your data*. Available at: https://www.which.co.uk/news/article/the-smart-device-brands-harvesting-your-data-al4vp6Z3ePDf (accessed 31 May 2025).
[41] ICO (2024) *Guidance on the use of storage and access technologies – draft impact assessment*. Available at https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/impact-and-evaluation/impact-assessment/guidance-on-the-use-of-storage-and-access-technologies-draft-impact-assessment-december-2024/ (accessed 31 May 2025).
[42] IAB (2023) *The Digital Dividend*. Available at: https://www.iabuk.com/news-article/digital-dividend-introduction-iab-uks-ceo-jon-mew (accessed 31 May 2025).
[43] Department for Business and Trade (2024) *Business Population Estimates*. Available at: https://www.gov.uk/government/statistics/business-population-estimates-2024 (accessed 31 May 2025).
[44] Which? (2024) *Why is my air fryer spying on me*? Available at: https://www.which.co.uk/policy-and-insight/article/why-is-my-air-fryer-spying-on-me-which-reveals-the-smart-devices-gathering-your-data-and-where-they-send-it-a9Fa24K6gY1c (accessed 31 May 2025).
[45] Anselmi et al (2024) *Watching TV with the Second-Party*. Available at: https://arxiv.org/pdf/2409.06203 (accessed 31 May 2025).

Samsung) for automated content recognition, finding that could operate even when the smart TV is used as a 'dumb' external display, when streaming from a second-party device for instance.

The range of concerns noted in relation to the operation of the consumer IoT products and services market include:

- Use of online tracking technologies and failure to obtain valid consent or provide clear and comprehensive information about the purposes of the online tracking technologies used.
- Bundling of consent for terms and conditions and the privacy policy into a single tick-box interaction as part of signing-up.
- Use of privacy policies that are overly long and inaccessible.
- Reliance on incorrect lawful bases, eg consent, to process personal information while not providing an opportunity to withdraw consent.
- Reluctance to act as joint controllers with organisations providing software development services.
- Lack of clarity on who should be responsible for processing as a controller, joint controller and processor.
- Inadvertent sharing of sensitive personal data with third parties in the IoT supply chain without proper safeguards.
- Mismatch between privacy settings available and the choices made on the use of personal data during set-up.
- Pre-selection of some privacy settings by default, for example for advertising.

Industry research has highlighted the challenges for IoT products and services,[46] in complying with data protection regulations, noting the following challenges and technical difficulties:

- 'Balancing compliance requirements with device capabilities'.
- Controlling 'security throughout their supply chain' either through 'vendor assessment processes, contractual security requirements' or 'ongoing monitoring'.
- 'Ensuring and documenting the security of each component' particularly due to the 'complex supply chains behind connected devices'.
- 'Implementing robust authentication mechanisms while maintaining usability and performance'.

2.4. Summary

Within this section we have defined IoT and consumer IoT products and services and set out the problem that our intervention aims to address using available research and evidence. We have used this evidence to estimate the size of the

[46] Finite State (2025) *How IoT Device Security Challenges Impact Regulatory Compliance*. Available at: https://finitestate.io/blog/iot-compliance-regulations-security-challenges (accessed 31 May 2025).

consumer IoT products and services market and identify some of the issues noted within this market in relation to privacy and data protection.

The information presented throughout this section is summarised in the box that follows to provide the problem statement the ICO aims to address with our intervention.

Problem statement

Much of the data processing in IoT products relates to tracking user activity. The Online Tracking Strategy identifies four areas where people are not being given the control they are entitled to under data protection law: deceptive or absent choice; uninformed choice; undermined choice; and irrevocable choice. These areas are present across a wide range of websites, services and technologies (including IoT devices), affecting nearly all adults online.

When users lack control, harm can occur. For example, people's private information, including sensitive biometric information, and location may be identified, causing unwanted disclosures and the potential for harm. However, it is recognised that there are particular problems for IoT products and services in complying with data protection legislation, for instance in the delivery of privacy information. ICO intervention is required to provide clarity on our regulatory expectations to organisations who process personal information in consumer Internet of Things (IoT) products.

3. Rationale for intervention

This section sets out the rationale for intervention and why the ICO is best placed to solve the problems identified in Section 2. It considers the political and legal context, the groups and individuals likely to be affected by the intervention, market failures this intervention seeks to address, actual and potential data protection harms, and the legislative basis for intervention.

3.1. The policy context

It is important to consider the wider policy context surrounding our identified problem to assess alignment with the rationale for intervention. This includes both internal ICO policy and wider initiatives such as government policy.

3.1.1. ICO policy

ICO25 is the ICO's overarching strategic plan.[47] There are four objectives of the strategy, with the most relevant to this intervention being objectives one and two, as follows:

- safeguard and empower people; and
- empower responsible innovation and sustainable economic growth.

ICO intervention is required, to contribute to achieving these objectives through the:

- provision of regulatory certainty and clarity to organisations on how data protection law and PECR apply when they process personal information in consumer IoT products; and
- reduction of the potential for data protection harms, through ensuring that personal (including special category) information is processed appropriately.

Within the ICO's response to government on economic growth,[48] and in line with the strategic enduring objective to empower responsible innovation and sustainable economic growth set out in our ICO25 strategic plan; the ICO has committed to supporting businesses and innovators to navigate the UK's regulatory landscape in their development and deployment of new technologies. In particular, the ICO committed to progress our pipeline of new and refreshed innovation-focused guidance, including on neurotech, cloud computing, and IoT products and services.

[47] ICO (2022) *ICO25 strategic plan.* Available at: https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/ (accessed 31 May 2025).
[48] ICO (2025) *ICO response to government on economic growth*. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/01/ico-response-to-government-on-economic-growth/ (accessed 31 May 2025).

Since 2019, the ICO has undertaken considerable work in the area of online privacy including:

- Guidance on consent or pay;[49]
- lawfulness, fairness and transparency guidance;[50]
- Guidance on the use of storage and access technologies;[51]
- Citizen jury on consumer IoT;[52]
- biometrics data guidance;[53]
- work to improve compliance with storage and access technologies guidance;[54]
- consumer guidance on smart products;[55]
- guidance on ensuring transparency in AI;[56]
- Privacy Enhancing Technologies (PETS) guidance;[57]
- action against Experian on how it handles people's personal data (taking account of subsequent case law rulings);[58]
- a joint paper with the CMA on harmful design;[59]

[49] ICO (2025) *Guidance on consent or pay.* Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/ (accessed 31 May 2025).
[50] ICO (2025) *Lawfulness, fairness and transparency*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/lawfulness-fairness-and-transparency/ (accessed 31 May 2025).
[51] ICO (2024) *Guidance on the use of storage and access technologies*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/online-tracking/ (accessed 31 May 2025).
[52] ICO (2024) *Citizen Jury on Consumer Internet of Things*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ (accessed 31 May 2025)
[53] ICO (2024) *Biometric data guidance*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/ (accessed 31 May 2025).
[54] ICO (2023) *Cookies letters project.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/commissioner-warns-uk-s-top-websites-to-make-cookie-changes/ (accessed 31 May 2025).
[55] ICO (2023) *Smart products*. Available at: https://ico.org.uk/for-the-public/online/smart-products/ (accessed 31 May 2025).
[56] ICO (2023) *How do we ensure transparency in AI*? Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-transparency-in-ai/ (accessed 31 May 2025).
[57] ICO (2023) *Privacy-enhancing technologies (PETs).* Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/ (accessed 31 May 2025).
[58] ICO (2024) *Action against Experian.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-statement-on-upper-tribunal-ruling/ (accessed 31 May 2025).
[59] ICO (2023) *Harmful design*. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/08/it-s-time-to-end-damaging-website-design-practices-that-may-harm-your-users (accessed 31 May 2025) .

- Commissioner's opinion on online advertising proposals;[60] and
- guidance on designing products to protect privacy.[61]

This work will also help to deliver on the areas of focus within the Online Tracking Strategy,[62] namely encouraging changes to ensure that:

- people can operate online with trust and confidence;
- people don't feel they have to contort their actions online to stay private and safe;
- people can meaningfully control who can use their information;
- people can meaningfully change how their information is used – especially if it's causing them distress or discrimination; and
- organisations are not disadvantaged by following the rules and improving their approach to online tracking to ensure it is compliant.

3.1.2. Relevant legislation

Any proposed regulatory intervention on consumer IoT products and services would be developed in accordance with relevant legislation, in particular PECR,[63] UK GDPR[64] and the Data Protection Act 2018 (DPA 2018).[65] These laws control how organisations, businesses or the government use personal information. Linked to the problem statement our intervention would provide clarification to organisations on the compliant and lawful processing of information gathered through consumer IoT products and services.

3.1.3. Relevant external policy landscape

Some of the relevant external policy considerations include:

[60] ICO (2021) *Opinion on online advertising proposals.* Available at: https://ico.org.uk/about-the-ico/what-we-do/information-commissioners-opinions/ (accessed 31 May 2025).
[61] ICO (various dates) *Designing products to protect privacy*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/ (accessed 31 May 2025).
[62] ICO (2025) *Taking control: our online tracking strategy*. Available at: https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/online-tracking-strategy/ (accessed 31 May 2025).
[63] UK Government (2003) *The Privacy and Electronic Communications (EC Directive)* Regulations 2003. Available at: https://www.legislation.gov.uk/uksi/2003/2426 (accessed 31 May 2025).
[64] UK Government (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Available at: https://www.legislation.gov.uk/eur/2016/679/contents (accessed 31 May 2025).
[65] UK Government (2018) *Data Protection Act 2018*. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 31 May 2025).

- New approach to ensure regulators and regulation support growth.[66] This action plan sets out the government's commitment to support growth through enabling a regulatory system that supports innovation and economic growth while ensuring accountability for the quality of regulations introduced, as well as the way in which independent regulators implement and enforce these regulations.
- Secure by design[67] sets out the government's ambitions in working to protect UK citizens, businesses the wider economy from the threats posed by poorly secured consumer connectable products.

Providing clarity and practical advice should help organisations to feel more confident about their use of personal data and assist with meeting the objectives listed.

3.2. Market failures

Our intervention seeks to help mitigate potential market failures around data protection and the non-compliant processing of personal information gathered through consumer IoT products and services. In this section we outline some of the potential market failures that may exist:

- **Information asymmetry**: When the extent and purpose of data collection by IoT devices is not sufficiently clear to consumers, for example they lack knowledge about how much or what kind of data is collected, how their data is used or the risk of breaches, consumers cannot make informed choices. This reduces the market pressure on firms to improve data protection compliance. Organisations within the consumer IoT ecosystem may not fully understand how personal data is being used along the supply chain further compounding the risks.
- **Negative externalities:** A poorly secured IoT devices is at greater risk of attacks by bad actors. Breaches may expose not only the device owner's data but that of other members of the household or house guests. As organisations within the consumer IoT ecosystem do not bear the full social cost of insecure devices, they may not fully account for these costs.
- **Underinvestment in security:** Data protection requires investment but the market rewards speed and low cost. Security is often invisible, and consumers may assume that all IoT products and service are sufficiently secure, making it hard for firms to compete on security.

[66] UK government (2025) *New approach to ensure regulators and regulation support growth*. Available at: https://www.gov.uk/government/publications/a-new-approach-to-ensure-regulators-and-regulation-support-growth/new-approach-to-ensure-regulators-and-regulation-support-growth-html (accessed 31 May 2025).
[67] UK government (2024) *Secure by design*. Available at: (https://www.gov.uk/government/collections/secure-by-design (accessed 31 May 2025).

- **Time inconsistent preferences:** Consumers may trade privacy for convenience, only to regret this decision later. This behavioural failure leads firms to exploit short term preferences over long term well-being.
- **First mover disadvantage:** Organisations within the consumer IoT ecosystem that invest in secure designs face higher upfront costs without guaranteed market rewards. Organisations that cut corners can undercut prices, pushing secure devices out of the market or into niche segments.
- **Inefficiencies in the supply chain:** A lack of clarity on how to comply with data protection law can result in inefficiently high costs for organisations, as they could incur costs in order to ensure they are complying with the law, such as seeking legal advice or the costs associated with legal or regulatory action.
- **Chilling effects:** A lack of security and transparency and increased risks of data breaches over the long term is likely to erode consumer trust in IoT devices. This could lead to consumers opting out of sharing data or stopping using device altogether. This diminishes the potential value of initiatives which depend on the processing of personal information.

3.3. Actual or potential harms

This section provides some illustrative examples of the harms in line with the evidence set out in Section 2.1, that can result from the non-compliant processing of personal information gathered through consumer IoT products and services.[68] This is a non-exhaustive list for illustrative purposes.

3.3.1. Loss of control of personal data and unwarranted intrusion

Harms may arise where there is loss of control of personal data, such as restrictions on a person's ability to access or review the use of their data, or through unwarranted intrusion such as unwanted advertising or surveillance.

Example: Loss of control of personal data and unwarranted intrusion

The FTC found that children's voice data obtained through the Alexa voice assistant was retained indefinitely on databases after deletion requests were received. Additionally, the option to delete geolocation data was found to ineffective, as while the data was deleted from some locations it was retained elsewhere. Thirdly, the FTC found that as the data gathering and storage approaches differed from those outlined when consent was sought, therefore invalidating the consent provided at that time and effectively obstructing the users' control over their personal data (and that of their children where relevant).

[68] ICO (2022) *Overview of DP Harms and the ICO's Taxonomy*. Available at: https://ico.org.uk/media2/about-the-ico/documents/4020144/overview-of-data-protection-harms-and-the-ico-taxonomy-v1-202204.pdf (accessed 31 May 2025).

This suggests personal data was gathered and stored without the users full knowledge or valid consent. Without knowing how and when data is being gathered and stored, users are likely to be subject to a loss of control of personal data.

3.3.2. Financial, bodily or psychological harm

Non-complaint use of IoT devices increases the risk of data protection harm to consumers. Where data security is breached, for example through hacking or a breach, personal data has the potential to lead to financial, bodily or psychological harm.

Example: Financial, bodily or psychological harm

The FTC found evidence of financial harm and psychological harm resulting from security failures at home security camera company Ring.[69] The FTC found that, due to insufficient controls, employees and contractors were able to access videos inside customer's homes. One employee accessed 'thousands of videos of female users in their bedrooms and bathrooms, including videos of Ring's own employees.' Further, the FTC states 'Ring's security failures ultimately resulted in more than 55,000 U.S. customers experiencing serious account compromises [up to January 2020].' Customers whose cameras were compromised, including children and older adults suffered from harassment and threatening behaviour for example:

- Hackers taunted several children with racist slurs;
- Individuals were sexually propositioned; and
- A hacker threatened a family with physical harm if they didn't pay a ransom.

3.4. Summary of rationale for intervention

In summary, the combination of compliance concerns, data protection harms and market failures have prompted the ICO to determine that action needs to be taken to improve regulatory certainty on how PECR and GDRP regulations apply to IoT products and services. Without regulatory intervention, firms are likely to continue to underinvest in data protection, consumers are likely to be exposed to increasing data protection risks over time and wider society is likely to face increased costs of harm mitigation.

[69] Federal Trade Commission (2023) *FTC says Ring employees illegally surveilled customers, failed to stop hackers from taking control of users' cameras.* Available at: https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users (accessed 31 May 2025).

4. Options appraisal

This section provides an overview of the options considered in relation to the problem defined in Section 2; and rationale for intervention identified in Section 3. Options were considered across the full range of light touch and more prescriptive regulatory interventions available to the ICO.

4.1. Options for consideration

In order to identify a potential list of options we must look at realistic and achievable solutions. However, there are several challenges in the consideration of options to address the need for regulatory certainty among organisations who process personal information in consumer Internet of Things (IoT) products and services, including:

- Difficulty in obtaining a full understanding of the key significant dependencies, priorities, incentives, and other drivers around the use of IoT products and services, and a need for regulatory influence within a rapidly evolving landscape.
- Need for consistency (where appropriate) with other regulatory approaches in order to ensure a level playing field for UK organisations and wider society.

By considering constraints and dependencies including the current draft guidance on the use of storage and access technologies[70] we can ensure all shortlisted options are both realistic and achievable. The options outlined are therefore not the full list of potential solutions, but rather those that are possible and realistic at this point in time. They provide a sense of the implications of alternative approaches and will provide a framework to demonstrate the rationale for deciding on the preferred option.

The options considered included:

Option 1: Business as usual: Provide no further intervention in relation to consumer IoT.

Option 2: Light-touch engagement: Adopt a light touch regulatory approach using education, engagement and influence.

[70] ICO (2024) *Guidance on the use of Storage and Access Technologies (draft).* Available at: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/ (accessed 31 May 2025).

Option 3: Light-touch guidance: Adopt a light-touch regulatory approach through support and guidance setting out ICO expectations across the wider IoT market.

Option 4: Prescriptive regulatory action: Adopt prescriptive regulatory action using consensual audits and/or investigative and corrective approaches.

Option 5: Light touch engagement plus guidance: Provide a light touch regulatory approach using education, engagement and influence; alongside support and guidance setting out ICO expectations across the wider IoT market.

Option 6: Light touch engagement and guidance plus prescriptive regulatory action: Provide a light touch regulatory approach using education, engagement and influence; alongside support and guidance setting out ICO expectations across the wider IoT market. To be followed with prescriptive regulatory action using consensual audits and/or investigative and corrective approaches where necessary.

4.2. Assessment of options against critical success factors

In line with HM Treasury guidance,[71] we have qualitatively assessed options against the following critical success factors (CSFs):

- **Strategic alignment**: Considers how options fit with ICO25 objectives/ strategic causes and the wider policy landscape.
- **Affordability**: Covers the financial impacts of options, including the cost for the ICO of delivering and maintaining these options (e.g. staff time and other resources).
- **Achievability**: Considers the viability of options as long-term solutions, and whether further action is likely to be required in the future.
- **Risks:** Considers the risks posed to the ICO, including legal and reputational risks (this includes the risks of the ICO being challenged on outdated guidance).
- **Impacts:** Considers whether options have a positive or negative impact on affected groups (including whether options reduce regulatory uncertainty or impose additional costs).

Table 6 summarises our assessment of the options against the CSFs. Each option has been assigned a red = negative, amber = neutral, or green = positive (RAG) rating against each CSF. A degree of judgement is used to score options against each of these factors. Accordingly, the assessment should be viewed as indicative.

[71] HMT (2020) *The green book*. Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020 (accessed 31 May 2025).

Table 6: Summary assessment of options

Option	Strategic alignment	Affordability	Achievability	Risks	Impacts
Business as usual	Negative (-)	Positive (++)	Negative (-)	Negative (-)	Negative (-)
Light-touch engagement	Neutral (+-)	Neutral (+-)	Neutral (+-)	Neutral (+-)	Neutral (+-)
Light-touch guidance	Neutral (+-)	Neutral (+-)	Neutral/ positive (+-)	Neutral (+-)	Neutral (+-)
Prescriptive regulatory action	Neutral/ positive (+-)	Negative (-)	Neutral (+-)	Neutral (+-)	Neutral/ positive (+-)
Light touch engagement & guidance	Positive (+)	Neutral (+-)	Neutral/ positive (+-)	Neutral (+-)	Neutral/ positive (+-)
Light touch engagement, guidance & prescriptive regulatory action	Positive (++)	Negative (-)	Positive (+)	Neutral /positive (+-)	Neutral/ positive (+-)

Source: ICO analysis.

Based on the assessment of options against the CSFs outlined, the preferred option at this time is **Option 5: Light touch engagement plus guidance.** This option involves the provision of a light touch regulatory approach using education, engagement and influence alongside the development of support and guidance setting out ICO expectations across the wider IoT market.

This option has no negative ratings and although it was ranked as neutral in relation to affordability and risks, this option ranked neutral/ positive in relation to strategic alignment, achievability and impacts. The preferred option aligns with ICO25 objectives and the external policy environment. The upfront cost to the ICO of producing guidance is expected to be offset by the impact of increased regulatory certainty for organisations and the reduced potential for data protection harms.

While Option 5 is considered to be the highest scoring option and as such is deemed the most appropriate option to progress at this time, we may need to reassess this position should the situation within the IoT sector evolve. For example, we may find a need for further future intervention beyond the scope of this project to deliver the desired level of outcomes and impacts.

5. Detail of proposed intervention

The overall aim of this intervention is to provide regulatory certainty to organisations who process personal information in consumer IoT products and services. In order to achieve this aim, the preferred option of **light-touch engagement** and **guidance** intervention has been chosen, as identified in the previous section.

This section provides an overview of the proposed intervention along with a theory of change for the intervention, which covers the change that light-touch engagement plus guidance is expected to bring about. The section concludes by providing an overview of the main groups expected to be impacted by the intervention.

5.1. Light touch engagement

In order to ensure that the guidance is read and fully understood by the target audience, engagement with stakeholders has been incorporated throughout the guidance development process. As noted in Section 3, a Citizen jury on consumer IoT was held in 2024,[72] and advice for the public using IoT devices,[73] was also updated.

As highlighted at the outset of this document and in line with the ICO's Consultation Policy,[74] and Policy Methodology,[75] the ICO is consulting on the draft guidance and this draft impact assessment. Responses to this consultation will be analysed and considered in the development of the final guidance. In parallel this draft impact assessment will be iterated further based on any changes and where respondents have provided relevant impact information.

The draft guidance is also to be publicly launched to ensure that we:

- encourage manufacturers and developers in attendance to read the draft guidance and share responses to the consultation; and
- strengthen relationships with key manufacturers, developers and trade bodies in attendance.

[72] ICO (2024) *Citizen Jury on Consumer Internet of Things*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ (accessed 31 May 2025).
[73] ICO (2023) *Smart products*. Available at: https://ico.org.uk/for-the-public/online/smart-products/ (accessed 31 May 2025).
[74] ICO (2025) *Consultation policy*. Available at: https://ico.org.uk/media2/0u4f42e1/consultation-policy.pdf (accessed 31 May 2025)
[75] ICO (2024) *The ICO's policy methodology*. Available at: https://ico.org.uk/media/about-the-ico/policies-and-procedures/4028535/policy-methodology.pdf (accessed 31 May 2025).

Further promotion of the draft and finalised guidance and related content will be considered, through our social media channels and other mediums as appropriate.

5.2. The guidance

The draft guidance explains how data protection law and PECR apply when processing personal information in consumer IoT products. The guidance is aimed at organisations who process personal information in consumer IoT products and services. It provides greater regulatory certainty by setting out what organisations must, should, and could do to comply with legislative requirements within the ICO's remit or relevant established case law.

The draft guidance covers the processing of personal information by organisations providing IoT products on the consumer market; including:

- home entertainment products (smart speakers, connected TVs, connected toys);
- home automation products (smart lights and lightbulbs, smart thermostats, smart home hubs);
- domestic appliances (smart fridges, smart ovens);
- wellbeing products (fitness trackers, smart watches, smart scales, sleep monitors);
- security and safety products (smart security cameras, smart doorbells, smart baby monitors);
- over-the-counter medical devices (smart fertility trackers with a device, smart blood pressure monitors, smart pulse oximeters); and
- peripheral products (smart keyboards, smart mice, smart headphones).

The guidance doesn't cover:

- connected and autonomous vehicles;
- smart meters;
- smart cities; or
- the use of IoT products in enterprise and industrial settings.

Also, the guidance specifically doesn't cover mobile phones; tablets; and computers.

The following topics are covered within the draft guidance:

- About this guidance.
- What information do IoT products use?
- How do we ensure accountability in IoT products?
- How do we apply a data protection by design and default approach?
- How do we ensure our IoT products process information lawfully?
- How should we tell people what we're doing?
- How do we ensure accuracy in IoT?

- How do we help people exercise their rights?

5.2.1. Overarching objectives

The overarching objective of the guidance involves the provision of **regulatory certainty** to organisations. The production of guidance for consumer IoT products and services, aims to help organisations provide people with meaningful control across the AdTech ecosystem; reduce the potential for data protection harms; and meet the objectives noted. These include:

- a level playing field of compliance amongst organisations is achieved;
- innovative alternatives are developed and implemented;
- privacy is designed in from the get-go;
- privacy is retro fitted where appropriate;
- organisations respect and adhere to people's choices;
- organisations limit the use and sharing of people's information to the appropriate purposes;
- the risk of data protection harms is reduced; and
- people feel information is safeguarded when using online services.

These objectives align with the problem identified and the rationale for intervention outlined in Sections 2 and 3, as well as with the ICO's organisational strategic objectives which are outlined within ICO25,[76] particularly to:

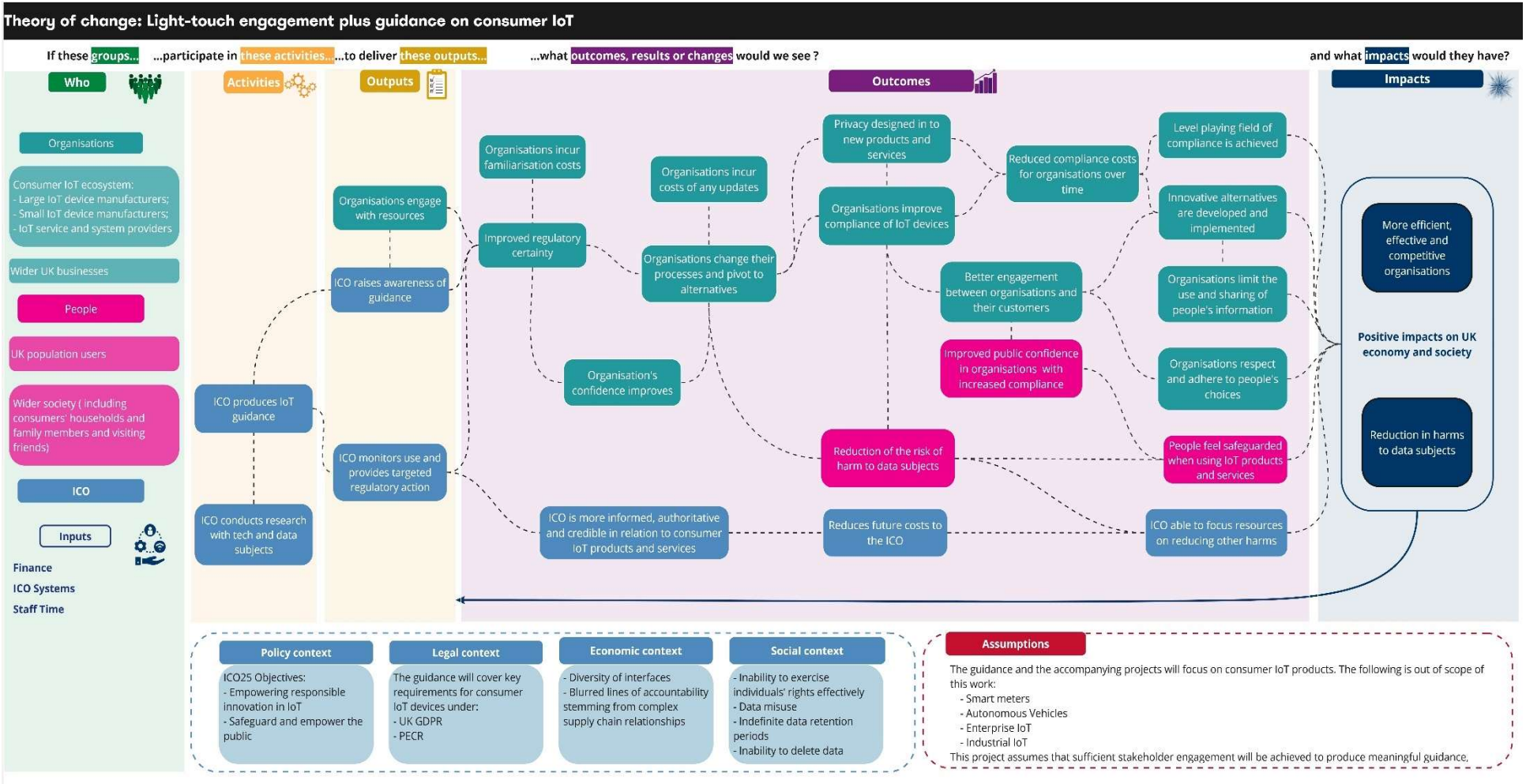
- safeguard and empower people; and
- empower responsible innovation and sustainable economic growth.

5.2.2. Theory of change

Our draft impact assessment is underpinned by an 'output to outcome to impact' methodology, called a theory of change. This shows how guidance can link to a chain of results that lead to the intended impacts. It should be noted that impact, linked to the rationale, is often the most difficult aspect to measure because it will occur over a longer period of time and can be influenced by other external factors. Our theory of change is shown in Figure 3.

[76] ICO (2021) *ICO25 strategic plan*. Available at: https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/ (accessed 31 May 2025).

Figure 3: Guidance on consumer IoT products and services – theory of change



Source: ICO analysis.

5.3. Scope of guidance

The draft guidance is primarily aimed at organisations who process personal information in IoT products. The guidance outlines the types of information that IoT products use; and sets out the ways that organisations can ensure accountability, process information lawfully, tell people what they're doing, ensure accuracy and help people exercise their rights.

5.4. Guidance timeline

The key milestones linked to the guidance from initiation to final guidance publication is illustrated in Figure 4.

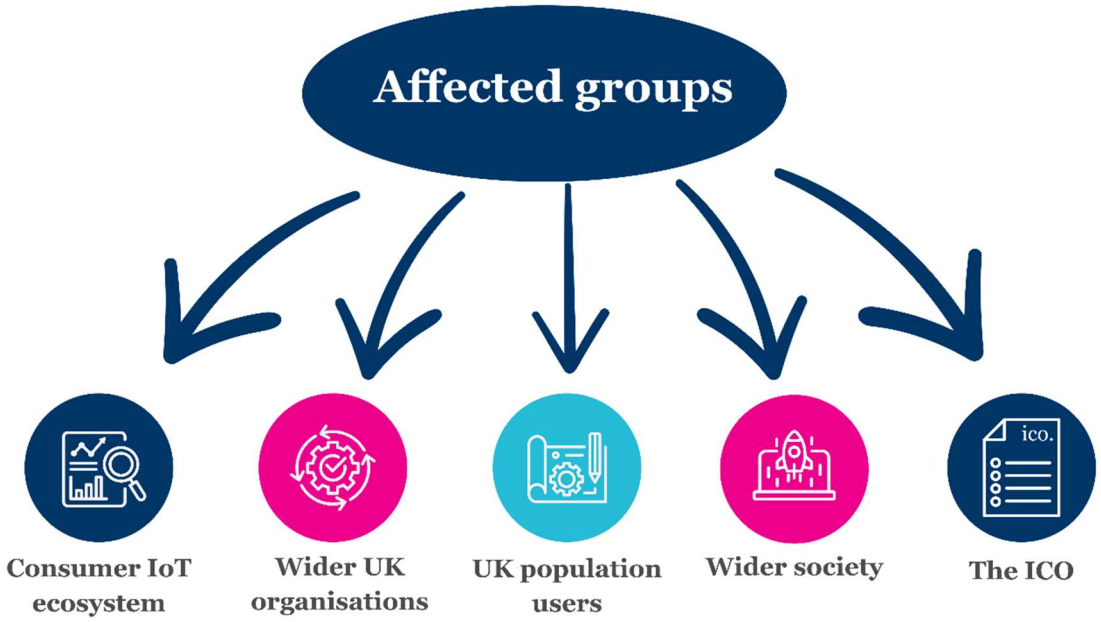
Figure 4: Timeline of key milestones linked to the guidance

Source: ICO analysis.

5.5. Affected groups

The main groups we expect to be affected by the guidance are outlined in Figure 5. There are a number of challenges with quantifying the scale of affected groups, including a lack of robust data and evidence as noted in Section 2.3. It is difficult to use official UK statistics and data on businesses (such as SIC codes which can be used to identify market size) to inform our understanding of the likely affected groups. Therefore, we have referred to a range of sources such as external research and surveys as noted in Section 2.3.

Figure 5: Affected groups



Source: ICO analysis.

5.5.1. Consumer IoT ecosystem

The guidance is expected to affect organisations across the consumer IoT ecosystem that process personal information in consumer IoT products and services. Such organisations are likely to include manufacturers, developers of operating systems, mobile app developers, web app developers, software developers, AI service providers, providers of biometric technologies, providers of sensors and telemetry, cloud providers, and cybersecurity and IT providers. These organisations are likely to be responsible for processing by IoT products; and so, may need a deeper understanding of how PECR and data protection legislation applies to processing of personal data in this sector.

It is noted that the guidance may impact organisations differently depending on their scale, role and influence within the sector, for instance:

- **Large IoT device manufacturers**: We expect that many of these manufacturers produce multiple IoT products and the majority of this group will have in-house capability to update themselves with standards outlined in the guidance. Further, we expect these firms to be interested in improving their compliance with existing legislation and therefore reduce the risk of future enforcement.
- **Small IoT device manufacturers**: This group, like larger manufacturers, will need to familiarise themselves with guidance. However, unlike larger manufacturers, these manufacturers may lack in-house capability to update existing processes due to dependencies on other product or service providers. However, we also expect these

manufacturers to be interested in improving their compliance with the guidance, in order to reduce the risk of enforcement in future.

- **IoT service and system providers**: These firms provide services that enable IoT functionality to devices. Typically, these firms will provide services to small IoT device manufacturers. Services are likely to include app or software development; cloud computing services; or app sales (such as app stores). This group will likely need to familiarise themselves with the guidance. They are also expected to see a reduction in the risk associated with potential future enforcement.

A 2023 OECD report[35] notes the difficulties in adequately measuring the number of IoT firms; estimating that around 13,000 innovative firms were operating in the global IoT market in 2021.

The IoT market is characterised by large players, with approximately 37% considered to be large organisations.

A complex ecosystem exists incorporating system components, system software and service providerss, device manufactureres, and connectivity technologies. Larger organisations may have many of these capabilities in-house, while this is unlikely to be the case for SMEs.

5.5.2. Wider UK organisations

Wider UK organisations are likely to be indirectly affected by the intervention due to the potential impacts of guidance in providing a more level playing field among across the consumer IoT ecosystem. It is anticipated that while few of these organisations may seek to understand the relevant legislation through engaging with guidance, they may benefit from the wider impacts of improved reputation through increased public confidence in organisational compliance with relevant legislation.

Given that IoT products and services process large amounts of often highly personal data about people who use them and people who are exposed to them, there is the potential for significant interaction between the use of IoT products and services and the online advertising sector as a whole.

The wider UK organisations that are likely to be affected, include those that receive data from device manufacturers and use data to target advertising at consumers. As a result of the guidance, these firms may be impacted by changes to the quantity of the data they receive from manufacturers and can therefore use to target consumers.

This has the potential to impact the perception of the effectiveness of any insights provided by data and may therefore lead to the potential reduction of revenue earned through personalised advertising and/or a shift towards other forms of revenue raising, such as non-personalised (known as contextual) advertising methods.

As outlined within our draft impact assessment on the use of storage and access technologies,[77] around 81% of SMEs that use paid-for online advertising say it is important to their business success, with 64% of UK SMEs (roughly 3.5 million organisations) having used some form of paid online advertising in the last year.[78]

According to UK business statistics there are approximately 5.5 million businesses across all sectors within the UK with around 3.5 million of those considered to be SMEs.[79]

5.5.3. UK population users

Consumers purchase IoT products and services which may collect personal data of the consumers, their households and house guests. As a result of the guidance, and subsequent improvements made to compliant processing among organisations within the consumer IoT ecosystem, this group is likely to experience a reduction in the quantity of their personal data which is shared with manufacturers. This is likely to reduce the risk of data protection-based harms for consumers and their households (as outlined in Section 3.3).

UK population users may also experience an increase in the price of IoT products and services as manufacturers seek to offset any loss made by making changes to their business models. They may experience a drop in the effectiveness of products as manufacturers may have less data to use to improve or align products and services with changes in consumer preference. Targeted advertising to these consumers may also become less effective, potentially increasing search costs for these consumers. However, through enabling a more level playing field of compliance across organisations, it is likely that guidance will result in an overall reduction in search costs for consumers.

[77] ICO (2024) *Guidance on the use of storage and access technologies – draft impact assessment*. Available at https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/impact-and-evaluation/impact-assessment/guidance-on-the-use-of-storage-and-access-technologies-draft-impact-assessment-december-2024/ (accessed 31 May 2025).
[78] IAB (2023) *The Digital Dividend*. Available at: https://www.iabuk.com/news-article/digital-dividend-introduction-iab-uks-ceo-jon-mew (accessed 31 May 2025).
[79] Department for Business and Trade (2023) *Business Population Estimates*. Available at: https://www.gov.uk/government/statistics/business-population-estimates-2023 (accessed 13 December 2024).

According to industry reports,[80] approximately 80% of the UK population (aged 16+) could be currently considered users of IoT products and services. This equates to approximately 45 million people.[81]

5.5.4. Wider society

Wider economy society refers to the whole of UK population, society, and economy. Due to the wide presence of IoT products such as smart speakers,[82] smart doorbells and smart security cameras, within and outside of households; the potential exists for the wider population of the UK to come into indirect contact with these devices, often without their knowledge.

This group is likely to benefit from a reduction in data protection harms as a result of guidance, through any improvements compliance across organisations and mitigation of harms. As firms adapt to the standards set out in the guidance there are likely to be costs in terms of increasing prices of IoT products and services. However, there may also be lower search costs for firms and consumers as transparency improves and a level playing field of compliance across organisations is encouraged.

We could assume that the entire UK population could be currently considered within the wider population of those potentially interacting with IoT products and services. This equates to approximately 68 million people.[81]

5.5.5. ICO

The ICO will be affected, as the regulator of data protection legislation and as the producer of the guidance.

This group is wholly represented by the ICO.

[80] Tech UK (2023) *State of the Connected Home*. Available at: https://www.techuk.org/resource/state-of-the-connected-home-2023) (accessed 31 May 2025).
[81] ONS (2024) *UK population mid-year estimate 2022*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates (accessed 31 May 2025).
[82] FTC (2023) *Out of the mouths of babes? FTC says Amazon kept kids' Alexa voice data forever – even after parents ordered deletion*. Available at: https://www.ftc.gov/business-guidance/blog/2023/05/out-mouths-babes-ftc-says-amazon-kept-kids-alexa-voice-data-forever-even-after-parents-ordered (accessed 31 May 2025).

6. Cost-benefit analysis

In this section we set out our initial assessment of the potential costs and benefits of the draft guidance on consumer IoT products and services.

- This cost-benefit analysis is a high-level outline of the potential impacts of the draft, which we have considered so far.
- It is important to note that we do not intend for this to provide an exhaustive assessment of impacts. It is an initial overview of considerations.
- We will develop this work further into a more detailed cost-benefit analysis as we move towards publication of the finalised guidance post-consultation.

We are seeking feedback on this draft assessment, as well as any other insights stakeholders can provide on impacts. This will allow us to iterate our impact assessment further to help inform our finalised guidance.

6.1. Identifying impacts – our approach

In identifying the potential impacts of the draft guidance, it is important to distinguish between:

- Impacts that can be attributed to the guidance. These are affected by how the ICO chooses to develop the guidance.
- Impacts that are not attributable to the guidance. These are impacts that simply arise from the existing legislative requirements that controllers are already expected to comply with.

For the purposes of the impact assessment, we are interested in impacts that are attributable to the draft guidance, rather than those that would have happened in the absence of regulatory intervention; a concept known as 'additionality'. Additionality can take a number of forms and may include the realisation of impacts at an earlier stage or to a higher scale or standard than would have been the case without intervention. Impacts can also be direct or indirect:

- Direct impacts: these are 'first round' impacts that are generally immediate and unavoidable, with relatively few steps in the theory of change between the introduction of the measure and the impact taking place.
- Indirect impacts: these are 'second round' impacts that are often the result of changes in behaviour or reallocations of resources following the immediate impact of the introduction of the measure. These impacts tend to be at the latter stages of a theory of change.

While it is not always feasible to categorise impacts distinctly, we have identified those that are attributable to guidance as far as possible. Our impact assessment draws on a mixture of quantitative and qualitative evidence where available, to substantiate and measure impacts. However, as discussed in more detail within Section 2, our analysis is limited by the lack of robust and specific evidence available.

6.2. Counterfactual

The counterfactual is a term used to describe the baseline or current level of activity. Measuring this baseline allows us to measure the additionality of introducing the guidance. As outlined in Section 4.1, Option 1: Business as usual reflects the counterfactual of our intervention of 'light-touch engagement plus guidance' and involves no further intervention in relation to consumer IoT.

6.3. Costs and Benefits

Table 7 gives an overview of the impacts on affected groups. Quantification in relation to both the scope (the size and scale of affected groups) and depth (the degree of change expected for entities within the affected groups) of costs and benefits has not been fully possible at this stage as evidence gaps and proportionality considerations have prevented a more comprehensive assessment.

As set out in the Treasury's Green Book,[83] it is necessary to consider the significant levels of uncertainty surrounding the evidential assumptions used to estimate the potential impacts of this draft guidance. This tests the sensitivity of impact estimates to changes in assumptions and is provided in Section 6.3.1.[84]

As noted at the outset, we will develop our analysis further as we move towards publication of the final guidance, based on information and feedback received through the consultation process.

[83] HMT (2020) *The green book*. Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020 (accessed 31 May 2025).
[84] See para 5.59 of HM Treasury's Green Book for more information on sensitivity analysis.

Table 7: Summary of potential impacts

Affected groups	Benefits	Costs
Consumer IoT ecosystem: Large IoT device manufacturers.	• Improved understanding of relevant legislation through engagement with the guidance. • Reduction in costs of obtaining alternative sources of advice and legislative understanding (eg legal advice). • Improvement in organisation confidence and therefore their ability to plan, invest, and operate more effectively. • Reduction in potential costs associated with over-compliance through enabling organisations to focus on the essential requirements of compliance. • Reduction in potential future costs of non-compliance with relevant legislation (eg avoidance of future intervention including enforcement and financial penalties), by enabling organisations to proactively address compliance issues, preventing costly mistakes or penalties.	• Familiarisation costs of engagement with the guidance (estimated to be approximately £125 per organisation).[85] • Implementation (and maintenance) costs of updates and introduction of compliant processes where necessary; potentially across multiple products and services. • Development and implementation costs associated with the design of new products and services with privacy 'designed in' from the beginning. • Research and development costs of creating innovative new processes, products, and services.

[85] Familiarisation costs are the costs associated with reading and becoming familiar with new or revised guidance. We calculate these as administrative costs associated with an individual at manager, director or senior official level reading the document. See Annex A for further detail on our approach.

	• Improved reputation of organisations through increased public confidence in organisational compliance with relevant legislation. • Provision of increased clarity around compliant processing of user data gathered by consumer IoT products and services, leading to a more level playing field among organisations within the consumer IoT ecosystem and wider UK organisations.	
Consumer IoT ecosystem: Small IoT device manufacturers.	• Improved understanding of relevant legislation through engagement with guidance. • Reduction in costs of obtaining alternative sources of advice and legislative understanding (eg legal advice). • Improved clarity on who should be responsible for processing as a controller, joint controller, and processor. • Improvement in organisation confidence and therefore their ability to plan, invest, and operate more effectively. • Reduction in potential costs associated with over-compliance through enabling	• Familiarisation costs of engagement with the guidance (estimated to be approximately £125 per organisation).[86] • Implementation (and maintenance) costs of updates and introduction of compliant processes where necessary; potentially across multiple products and services or in alignment with externally produced products and services. • Development and implementation costs associated with the design of new products and services with privacy 'designed in' from the beginning.

[86] Familiarisation costs are the costs associated with reading and becoming familiar with new or revised guidance. We calculate these as administrative costs associated with an individual at manager, director or senior official level reading the document. See Annex A for further detail on our approach.

	organisations to focus on the essential requirements of compliance. • Reduction in potential future costs of non-compliance with relevant legislation (eg avoidance of future intervention including enforcement and financial penalties), by enabling organisations to proactively address compliance issues, preventing costly mistakes or penalties. • Improved reputation of organisations through increased public confidence in organisational compliance with relevant legislation. • Provision of increased clarity around compliant processing of user data gathered by consumer IoT products and services, leading to a more level playing field among organisations across the consumer IoT ecosystem and wider UK organisations.	• Research and development costs of creating innovative new processes, products, and services.
Consumer IoT ecosystem: IoT service and system providers.	• Improved understanding of relevant legislation through engagement with guidance. • Reduction in costs of obtaining alternative sources of advice and legislative understanding (eg legal advice).	• Familiarisation costs of engagement with the guidance (estimated to be approximately £125 per organisation).[87] • Implementation (and maintenance) costs of updates and introduction of compliant device functionality where necessary; in alignment

[87] Familiarisation costs are the costs associated with reading and becoming familiar with new or revised guidance. We calculate these as administrative costs associated with an individual at manager, director or senior official level reading the document. See Annex A for further detail on our approach.

- Improved clarity on who should be responsible for processing as a controller, joint controller, and processor.
- Improved clarity on who should be responsible for processing as a controller, joint controller, and processor.
- Improvement in service and system providers' confidence and therefore their ability to plan, invest, and operate more effectively.
- Reduction in potential costs associated with over-compliance through enabling service and system providers to focus on the essential requirements of compliance.
- Reduction in the risk of potential future costs of non-compliance with relevant legislation (eg avoidance of future intervention including enforcement and financial penalties), by enabling organisations to proactively address compliance issues, preventing costly mistakes or penalties.
- Provision of increased clarity around compliant processing of user data gathered by consumer IoT products and services, leading to a more level playing field among organisations across the consumer IoT ecosystem and wider UK organisations.

with the requirements of small IoT device manufacturers.

- Development and implementation costs associated with the design of new products and services with privacy 'designed in' from the beginning.
- Research and development costs of creating innovative new processes, products, and services.

Wider UK organisations.	• Improved reputation through increased public confidence in organisational compliance with relevant legislation. • Organisations may pivot to other privacy enhancing models of revenue raising such as contextual advertising. • Provision of increased clarity around compliant processing of user data gathered by consumer IoT products and services, leading to a more level playing field among organisations within the consumer IoT ecosystem and wider UK organisations.	• Potential perceived reduction in the effectiveness of insights and consumer targeting, due to a reduction in the amount of personal data available. • Potential reduction in revenue for organisations that generate income through personalised advertising. • Potential reduction in market size and potential due to impacts on organisations that generate income through online advertising; or use/rely heavily on online advertising markets. • Organisations may pivot to other models of revenue raising.
UK population users.	• Access to better and more compliant consumer IoT products and services. • Improved ability to exercise data protection rights both from increased knowledge of relevant legislation and access to more compliant consumer IoT products and services. • Reduction in potential data protection harms. • Improved engagement with organisations. • People feel safeguarded when using IoT products and services. • Reduction in search costs for consumers through more level playing field of compliance across organisations.	• Potential for increased friction due to potential changes in consent management practices by organisations. • Potential reduction in service offerings due to reduced profitability of organisations that use/rely on online advertising markets. • Potential increase in price of IoT products and services, where manufacturers pass on costs of compliance to customers.

Wider society.	• Improved ability to exercise data protection rights both from increased knowledge of relevant legislation and access to more compliant online services. • Reduction in potential data protection harms. • People have greater trust in the compliance of organisations that are processing data gathered through their use or interaction with consumer IoT devices (either with or without their knowledge).	• Potentially reduced wider organisational service offerings or the removal of a service altogether.
ICO.	• Ability to allocate resources efficiently.	• Upfront resource costs.

Source: ICO analysis.

6.3.1. Key Assumptions

The impacts identified at this initial impact assessment stage, from the intervention of light-touch engagement plus guidance are contingent on:

- organisations' awareness of the guidance;
- the extent that organisations engage with the guidance; and
- changes that are made to organisational practices as a result of engaging with the guidance.

While we are unable to quantify the impacts of these uncertainties, Table 8 provides an indication of the sensitivity of key impacts to these unknowns.

Table 8:Sensitivity of key impacts to identified risks

Impacts	Sensitivity
More efficient, effective, and competitive organisations.	Medium
Familiarisation costs for organisations.	High
Improved compliance with relevant legislation.	Medium
Implementation and maintenance costs for organisations.	High
Increased public trust and confidence.	High
Reduction in harms to UK data subjects.	Medium

Source: ICO analysis.

6.3.2. Initial assessment of impact

This initial draft assessment has identified a number of impacts of the draft guidance including the reduced potential for data protection harms. The guidance is expected to increase regulatory certainty for organisations within the consumer IoT ecosystem. Although there will be costs to organisations from reading, understanding, and implementing the guidance, this is expected to be outweighed by the wider societal benefits of reduced data protection harms.

At this draft stage of guidance development, we expect the guidance to have a net positive impact on balance. However, we will seek to gather additional information on the potential costs and benefits of the guidance throughout consultation and development of our final guidance and impact assessment.

Table 9 presents a summary of the main impacts we expect to see from the guidance at this point in time.

Table 9: Overall impacts of guidance on consumer IoT products and services

Impacts		Attribution to the ICO	Direct or Indirect
Benefits	More efficient, effective, and competitive organisations.	Partly Attributable	Indirect
	Improved compliance with relevant legislation.	Partly Attributable	Indirect
	Reduced data protection harms leading to increased public trust and confidence.	Partly Attributable	Indirect
Costs	Familiarisation costs of engaging with guidance.	Attributable	Direct
	Implementation and maintenance costs of deploying alternatives.	Partly Attributable	Indirect

Source: ICO analysis.

7. Monitoring and evaluation

As per our impact assessment framework, when finalising the guidance post consultation, we will consider the monitoring and review processes. As noted at the outset of this IA, this intervention sits within our wider Online Tracking Strategy.[88] As such the outcomes and impacts of this intervention will feed into any wider ex-post impact measurement carried out on the Online Tracking Strategy.

For example, this could include:

- Establishing a central monitoring system to review all outputs and outcomes within the theory of change, which is the minimum evidence required to measure early-stage outputs and provide some evidence of outcomes;
- Conducting post-engagement surveys with organisations engaged with upstream to understand improvements to their understanding and use of personal data for IoT products and services; and
- Exploring opportunities to monitor public understanding and comfort around the use of their personal data by IoT products and services.

[88] ICO (2025) *Our strategy for levelling the playing field for online tracking in 2025.* Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/01/our-strategy-for-levelling-the-playing-field-for-online-tracking-in-2025/ (accessed 31 May 2025).

Annex A: Familiarisation costs

This annex sets out the approach taken to estimate familiarisation costs for the guidance, which follows an approach drawn from our impact assessment guidance[89] and in line with government guidance.[90]

A.1 Familiarisation costs per organisation

We have estimated the total time for reading the guidance at 3 hours and 59 minutes. This is based on a word count of around 17,927 words and a Fleisch reading ease score of 36.5.

Table A.1: Estimate of the average time taken to read the guidance

Document	Word Count	Fleisch reading ease score	Assumed words per minute	Estimated reading time (hr:mn)
Guidance	17,927	36.5	75	3h59

Source: ICO analysis.

The impact of familiarisation on organisations can be monetised using data on wages from the ONS Annual Survey of Hours and Earnings.[91]

Making the conservative assumption that the relevant occupational group is 'Managers, Directors, and Senior Officials', the 2024 median hourly earnings (excluding overtime) for this group is £26. This hourly cost is uprated for non-wage costs using the latest figures from the Regulatory Policy Committee guidance,[92] resulting in an uplift of 22% and an hourly cost of £31. We therefore assume the cost of reading the guidance once to be approximately £125.

[89] ICO (2023) *The ICO's Impact Assessment Framework*. Available at: https://ico.org.uk/media/about-the-ico/documents/4027020/ico-impact-assessment-framework.pdf (accessed 31 May 2025).
[90] BEIS (2017) *Business Impact Target: Appraisal of guidance: assessments for regulator-issued guidance*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609201/business-impact-target-guidance-appraisal.pdf (accessed 31 May 2025).
[91] Office for National Statistics (2024) *Annual Survey of Hours and Earnings*. Available at:https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/bulletins/annualsurveyofhoursandearnings/2024 (accessed 31 May 2025).
[92] RPC (2019) *RPC guidance note on 'implementation costs'*. Available at: https://www.gov.uk/government/publications/rpc-short-guidance-note-implementation-costs-august-2019 (accessed 31 May 2025).