



Citizen Jury on Consumer Internet of Things

Prepared for the Information Commissioner's Office
by Impact Research

April 2024

ico.
Information Commissioner's Office

IMPACT
FROM INSIGHT TO INFLUENCE

Table of Contents

Foreword.....	2
Executive Summary.....	3
About this research.....	3
Participant perceptions.....	3
Recommendations for the ICO	5
What is Internet of Things?.....	7
Methodology.....	8
Findings	14
Before the workshops.....	14
During the workshops.....	15
Privacy and security when setting up an IoT product.....	17
Considering privacy while using an IoT product	25
Protecting your privacy when disposing of IoT products	31
Conclusion.....	34
Appendices.....	35
About Impact	44

Foreword

In 2022, as part of its Tech Horizons Report, the Information Commissioner's Office (ICO) committed to providing guidance on the Internet of Things (IoT) and regulating the processing of personal information through these technologies. This guidance will be designed to encourage responsible innovation in IoT and to safeguard the public.

There is little evidence in the public domain from recent years about how the public feels about IoT products and personal information. The ICO wanted to undertake participant engagement to:

1. Understand how the public perceives IoT products, and what they understand about processing of their personal information;
2. Understand the public's conditions and 'red lines' when incorporating IoT products into their personal lives;
3. Uncover the public's expectations from the ICO and product manufacturers;
4. Identify any related issues that may concern participants that are not currently in the ICO's plans.

This report represents the views of the Citizens' Jury on Internet of Things, which took place in the form of two online workshops in February 2024 that considered the Information Commissioner's Office's proposals for guidance on consumer IoT.

Executive Summary

About this research

In February 2024 the Information Commissioner's Office (ICO) and Impact Research worked together to ask the members of the public for their views on the propositions for ICO's guidance on the Internet of Things (IoT).

Impact Research recruited a demographically diverse group of 22 participants in January and February 2024 with the support of BEAM Fieldwork, a market research field specialist. Throughout two online workshops, we discussed experience with IoT products and common challenges related to their privacy and security. Participants provided feedback on areas related to the use and regulation of IoT products and made a series of recommendations to the ICO.

Participant perceptions

Participants grew more concerned about privacy and security of IoT over the course of the workshops.

Prior to the workshops during the initial engagement, participants did not spontaneously recognise the collection and processing of personal information as areas of concern. Many participants trusted manufacturers and generally felt comfortable with their personal information being collected, however, some expressed reservations. Only a few participants took proactive steps to protect their privacy and security, for example by using random password generation, providing incorrect personal information or using a virtual private network (VPN).

As participants became more informed throughout the workshops about how IoT products handle personal information, they became increasingly sceptical about entrusting their personal information to IoT products and the companies behind them.

Participants discussed how privacy and security measures could be introduced throughout the lifecycle of IoT products.

The overwhelming feeling among participants was that IoT products collect an excessive and often unnecessary amount of personal information. Most participants in this research live busy lives and therefore prioritised ease of setup and use, preferring minimal barriers to operation upon acquiring these products. This led them to ask for more clarity about what happens to personal information throughout the IoT product lifecycle, and how to access, move and delete data at any stage of the product lifecycle.

Participants are unclear about privacy and security features before purchasing.

- They assume products are secure when they buy them, and that household brands will apply best practices to keep their personal information secure.

- Encryption, while valued, wasn't always a determining factor in purchase decisions due to limited awareness about which IoT products offer it.

Participants find it hard to engage with privacy information and consent choices during setup and make choices on behalf of others.

- The process of giving consent and reading privacy information during setup is too long, complex, and lacks clarity. Privacy policies can often be overwhelming, and difficult to understand and remember.
- Participants identified that processes for getting consent and providing transparent information are limited to the initial setup and can be overlooked if they are not presented at convenient times.
- While participants acknowledged the benefits that profiling for personalisation can offer, they also called for greater transparency, simpler controls, and assurances that personal information is used responsibly. These mitigations were even more important to them when discussing the possibility of their information being shared with third parties for advertising.
- Some participants limited their use of certain smart features or products altogether if they felt they could infringe too much on their privacy.
- Few participants had direct experiences of setting up additional users for their IoT products (for example on smart speakers or doorbells). However, they recognised that while it is important for people who use and live around these products to have a say in how they use their personal information, it could be difficult to gain consent from all potential users during setup.

Participants didn't tend to think about privacy after setting up IoT products, but they did voice concerns about data sharing with other household members.

- Very few participants had tried to withdraw their consent from an IoT product.
- While participants appreciated the unobtrusive nature of IoT products, they agreed they would like the products to signal when they collect and use personal information; however, the signalling shouldn't be too disruptive to their lives.
- Most participants lacked confidence in their ability to access personal information from IoT products. Although they liked knowing they can access their information, they were unsure about what they would do with it.
- Participants raised several instances where sharing information within the household could be an issue:

- a) situations where household members use IoT products to harm and coercively control other members;
- b) when products which collect audio, like smart speakers and doorbells, making their conversations and queries available to the whole household.

Participants generally don't consider privacy when disposing of IoT products and are sceptical when they do try to delete information.

- Participants didn't find accessing their information very relevant to their experience; however they did see the necessity of deleting information, especially when they shared products with other household members or sold products to new owners.
- Some participants had tried to delete data but were sceptical about whether manufacturers retained personal information even after the supposed deletion. They avoid handing down IoT products to family and friends to prevent accidentally sharing their information.

Recommendations for the ICO

These recommendations were developed through facilitated discussions in smaller groups to ensure that we captured a range of views from all participants. The recommendations are a collection of conclusions rather than a group consensus and they are not in any particular order of importance. We have broadly categorized them according to areas of data protection regulation. Participants' recommendations are for manufacturers of IoT products and should serve as considerations for the ICO when developing their guidance. The recommendations should be considered in line with their technical feasibility as well as the scope of the law.

Security	<ul style="list-style-type: none"> • Manufacturers should be transparent upfront about whether the IoT product uses encryption and state the encryption standard. • Biometric data (voice, face scans, fingerprints) should always be encrypted and subject to additional security measure where necessary. • Manufacturers should consider implementing additional security measures such as two-factor authentication and notifications when signing into a product account from a new device.
Transparency information	<ul style="list-style-type: none"> • Manufacturers should make information about what data is collected and how it is used available at different stages of the product lifecycle, not just during setup. For example, before purchasing IoT products and periodic reminders at relevant moments. • Privacy policies should be clear and easy-to-understand, including categorisation of privacy information, the inclusion of visuals, bullet points, collapsible lists, and large text. • Where possible, manufacturers should incorporate audio or visual signals which would indicate when a product is collecting or using personal information. The signalling should be balanced against causing nuisance to people's lives.

<p>Consent & control</p>	<ul style="list-style-type: none"> • Manufacturers should consider implementing consent mechanisms that are offered at appropriate times throughout the product lifecycle, for example when there is a security update, a new user is added to the product or a periodic reminder of what they have consented to. • Manufacturers should provide easy-to-find settings for people to review and adjust their consent preferences including how to withdraw consent. This should be available to all who use an IoT product where possible. • Manufacturers should consider ways to give all users of shared IoT products control over their personal information. For example, by gaining collective consent on behalf of the household and applying a tiered hierarchy of control between different account holders. • IoT products with multiple users should have a 'guest mode' where capturing personal information can be paused for a desired time. This feature would be useful when non-members of the household who didn't consent to capture their personal information interact with products.
<p>Profiling & advertising</p>	<ul style="list-style-type: none"> • Manufacturers should give people granular controls to tailor what types of information are used for profiling throughout the product experience, not just during setup. • Specifically for advertising, the jury would like to see a prominent stand-alone control to opt-in to use of their personal information for this purpose. • If using personal information from an IoT product for advertising, manufacturers should clearly explain how they use the most sensitive information types to facilitate it. The jury considered health metrics from their fitness trackers to be sensitive as well as location data and financial information.
<p>Individual rights</p>	<ul style="list-style-type: none"> • Manufacturers should give people easy ways to delete their personal information from their IoT products, such as options in settings or automatic deletion of some information after a certain period. • Manufacturers should be clear about what happens to the personal information after people 'delete' it through the settings on the product. • Manufacturers should respect the request to move personal information to another IoT provider and delete all the information they hold about the people using the product once the transfer is completed. • Manufacturers should give owners of IoT products information about non-registered users and whether they can exercise their rights. They should make it clear in what situations they can request their information to be deleted, for example, as a passerby on the street interacting with a doorbell or a house guest interacting with a smart speaker.
<p>Accountability</p>	<ul style="list-style-type: none"> • In the future when people have to manage many more IoT products, manufacturers should work on developing a system which would allow people to control all of their IoT products at home.

What is Internet of Things?

The terms smart technologies, Internet of Things, IoT and connected products are often used interchangeably.

The Internet of Things describes the network of physical objects ('things') that can connect and share information with other things and systems over the Internet. These 'things' can sense, respond to or interact with the external environment, powered by a large range of technologies (for example, biometric or environmental sensors, artificial intelligence). IoT products process large amounts of often highly personal information about people who use them and people who are exposed to them.

IoT products can be used in many settings. For example, by:

1. people monitoring their wellbeing,
2. people managing their homes and setting up entertainment,
3. organisations monitoring their employees,
4. hospitals treating patients,
5. schools educating children,
6. factories managing effective production of products,
7. cities to measure traffic and how busy certain areas are.

For this research, we informed participants that we are only interested in the use of IoT products which would fall under points 1) people monitoring their wellbeing and 2) people managing their homes and setting up entertainment.

We also provided examples of some of the products they might have come across that fall within the scope of this research. For example, smartwatches, fitness trackers, smart kettles, thermostats, doorbells, smart TVs, and smart speakers.



Methodology

To answer ICO's objectives, Impact conducted qualitative research in the form of two workshops, each lasting 2 hours, and taking place online via Zoom. The workshops were carried out by Impact's team of moderators. The same group of participants and team of moderators attended both workshops.

Throughout the research process, we wanted to understand how participants felt about the IoT products used or shared in their households. We were mainly interested in IoT products that people use to monitor their wellbeing (smartwatches, fitness trackers, etc.) or products that people use to manage their homes and set up entertainment (thermostats, doorbells, smart TVs, and smart speakers). Despite focusing on IoT products, smart mobiles, mobile apps, social media, and general internet browsing experiences were still frequently top of mind. We didn't stop participants from mentioning these topics to allow them to express their lived experiences fully.

To get people to think about the issues with privacy and security we got a consumer expert from Which? to provide a balanced view about the pros and cons of IoT products and to share findings from their research.

We also wanted to gauge participants' attitudes and behaviour expectations relating to six specific areas of data protection regulation – consent, transparency, profiling and advertising, data sharing, accountability, and security. We presented the participants with propositions for the guidance developed by the ICO. We explained to them that the guidance is meant for manufacturers of IoT products and instructed them to provide feedback and recommendations on guidance propositions.



Areas of guidance and explored propositions

The table below shows headlines of guidance propositions we presented to participants during the Workshop 2. The complete list of guidance propositions created by the ICO can be found in Appendix C. The propositions were written using accessible language and concepts familiar to the general public rather than expert data protection terms.

Throughout this report, we didn't refer to the propositions in the order they were presented to participants. Based on the group discussions, we analysed participants' feedback on the propositions following an IoT product lifecycle – product setup, use and disposal.

<p>SECURITY Security of IoT products</p>	<p>Although not all personal information needs to be encrypted, companies should encrypt any information which is classed as 'special category' (voice, face scans, heartbeat or gait).</p>		
<p>TRANSPARENCY & CONSENT Making choices about personal information</p>	<p>Manufacturers should consider moments throughout the product lifecycle where it might be appropriate to show privacy information. They should consider how to ensure everyone can access privacy information when they need it even if they didn't set up the product.</p>	<p>Manufacturers should make it easy for people to understand what their consent is for, why it is required and how to change it at a later date. Manufacturers should consider moments throughout the lifecycle of the IoT product where people who use it may need to give/ change their consent.</p>	<p>Manufacturers must make it easy for everyone who gives consent for an IoT product to use their personal information to withdraw their consent at any time.</p>
<p>PROFILING Making product features and advertising specific to you</p>	<p>Manufacturers wanting to share or sell information for advertising must ask people for their consent. They should provide granular options for what type of personal information from an IoT product can be shared for advertising.</p>	<p>Manufacturers must give people details about: The categories of information they hold (for example, contact details, interests or special category information - political views & religion). The source of their information (for example, the organisation it came from).</p>	
<p>INDIVIDUAL RIGHTS Your rights over your personal information</p>	<p>IoT manufacturers must allow everyone who shares personal information with an IoT product, regardless of whether they are the registered owner or not, to exercise their rights.</p>	<p>IoT manufacturers should ensure that they have easy ways for people to request their information from IoT products to be moved to a different company.</p>	<p>It should be obvious when an IoT product is collecting personal information, especially when the product is not in direct use.</p>
<p>DATA SHARING Sharing information with your household</p>	<p>Manufacturers should provide flexible settings for individuals to share different levels of personal information with others who use the IoT product.</p>		
<p>ACCOUNTABILITY What happens when things go wrong with more than one IoT product</p>	<p>Manufacturers must provide clear information about all the partners and suppliers who have access to or control over people's personal information. They should also make it clear what type of information they hold and what to do if something goes wrong</p>		

The research included three polling exercises to gauge:

1. The level of knowledge about how technology companies/ manufacturers of IoT products use people's personal information,
2. The level of trust in technology companies/manufacturers of IoT products to keep people's information safe.
3. Areas of guidance that participants want ICO to prioritise.

The first two poll questions were repeated at the beginning and the end of each workshop, to track how much participants' perceptions of knowledge and trust have changed, if at all.

The prioritising polling exercise ran at the end of the second workshop after the participants received information about privacy and security challenges and the propositions for manufacturer guidance to allow them to make an informed choice.

The research consisted of the following stages:



Recruitment

A representative sample of UK consumers (also including some people who self-identified as experiencing some type of vulnerability themselves or are looking after someone vulnerable)¹ of 24 consumers was recruited by BEAM Fieldwork, Impact's trusted field partner. Of the 24 recruited, 22 completed both workshops and were incentivised for their time.

We spoke to the following respondent profiles.²

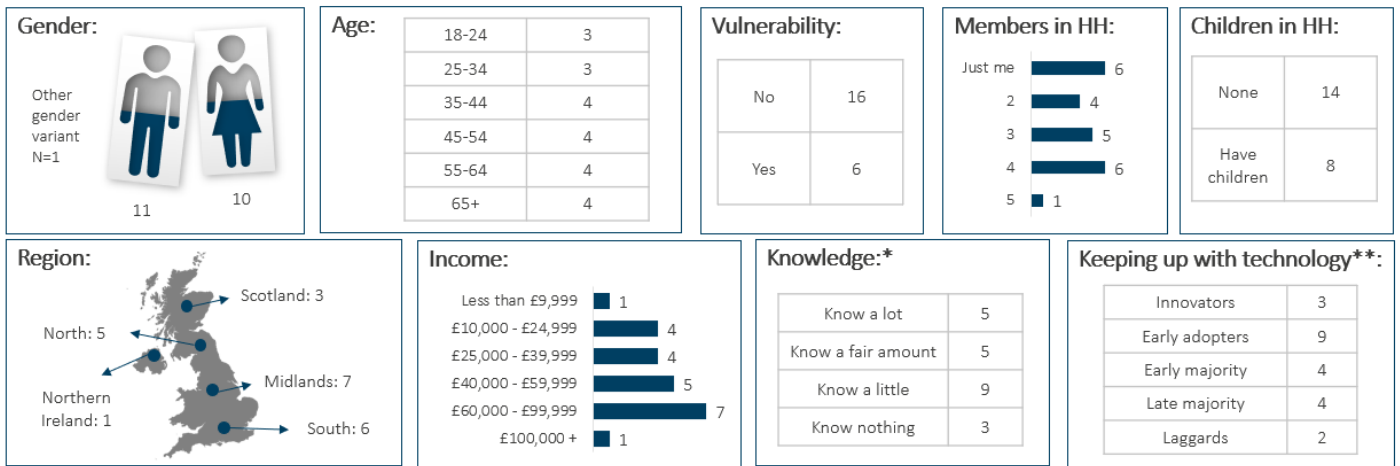
¹This included the following:

- I struggle to keep up with the money I owe to different companies and organisations
- My income is unpredictable; sometimes my income does not cover my cost of living
- I struggle to manage my finances
- It is difficult for me to keep in control of my money
- Sometimes my income does not cover my cost of living
- Where I live, it is difficult to access the things to support my basic needs
- My living conditions sometimes lack safety and stability;
- I am an unpaid carer for someone who relies on my support
- I experience addiction to substances or behaviours
- I sometimes feel left out or treated unfairly due to my race, ethnicity, gender, or sexual orientation

²*Knowledge about security, privacy and regulations of data stored or shared through smart products – we excluded people who classed themselves as experts

** Keeping up with technology: segment definitions:

- Innovators: I like to be one of the first people to have a new tech gadget
- Early adopters: I'm not always the first to buy a new gadget, but I tend to buy it before most others
- Early majority: I prefer for other people to prove out the technology gadget before I buy it myself
- Late majority: I prefer to wait until the price drops to buy a new technology gadget
- Laggards: I'm usually one of the last people I know to buy a new tech gadget



Participants were split into 4 smaller groups for workshop breakout rooms to discuss the different topic areas and propositions in more detail. We based the dividing criteria on demographics and vulnerability, to allow them to interact with those in a similar life stage/ situation to themselves.

- Group 1: self-identified as vulnerable
- Group 2: aged between 18-34
- Group 3: aged between 35-54 and/or have a family
- Group 4: aged 55+

Within each of the groups, there was a mixture of gender, region, household incomes, knowledge levels of privacy and security of smart products and the amount they kept up with new technology.

WhatsApp Task

Upon recruitment Impact engaged with participants through WhatsApp to build rapport and gain a basic understanding of attitudes to IoT products used in their households.

We asked recruited participants to answer three WhatsApp tasks in advance of the first workshop:

- Take pictures of smart products they have in the household – what they like and dislike about using them, and who uses them?
- Share a video about how they feel about information being collected while using such products.
- Did they take any precautions during the setup of the product or when using it?



Photos of IoT products participants have in their homes

Workshop 1

Workshop 1 took place on the 6th February 2024, it lasted 2 hours and consisted of the following discussion topics:

- Introductions to the IoT research and agenda
- First voting exercise (knowledge of the use of personal information and trust in tech companies)
- Introduction to what is IoT
- Introduction to the ICO
- Introduction to the first 3 areas detailed through videos from an industry expert Andrew Laughlin³ at Which?⁴
- Breakout room session 1 discussing the first three guidance areas
- Back to the main room for feedback on discussions
- Breakout room session 2 discussing remaining guidance areas
- Back to the main room for feedback on discussions
- Second voting exercise (knowledge of the use of personal information and trust in tech companies)
- Summary/ next steps

Propositions pre-read

After workshop 1, respondents were sent propositions developed by the ICO (see Appendix C) to read through before the start of the second workshop. There were 10 propositions in total.

Workshop 2

Workshop 2 took place on the 15th February 2024, it also lasted 2 hours and consisted of the following discussion topics:

- Introductions to workshop 2 and agenda
- First voting exercise (knowledge of the use of personal information and trust in tech companies)
- Summary of what was learnt in the first workshop and if they changed behaviours as a result
- Check if they read the propositions
- ICO introduction to the purpose of the guidance
- Brief introduction to the first 5 propositions
- Breakout room session 1 covering the first 5 propositions
- Back to the main room for feedback on discussions

³ ICO and Impact Research collaborated with Andrew Laughlin (a Principal Researcher & Writer) at Which?. Andrew helped us to co-create video stimuli to introduce the 6 research areas using consumer-friendly language and real-life examples. See Appendix B.

⁴ Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that influences politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation, we're not for profit and all for making consumers more powerful.

- Breakout room session 2 covering the next 5 propositions
- Back to the main room for feedback on discussions
- Second voting exercise (knowledge of the use of personal information, trust in tech companies and priority guidance areas)
- Summary

Analysis approach

Impact conducted a thematic analysis to identify key patterns and themes from both workshops. Firstly, we pulled out responses to the research objectives and any interesting points/ patterns. We then identified and created a list of codes (by highlighting transcripts and notes) to describe the content. We looked at the codes generated and grouped them based on similarities/ themes coming out in the data. We made notes of any quotes or recordings which we wanted to include in the report as supporting evidence.

Qualitative research is not always about the number of times something is mentioned, a point may have only been made by one person, but it may be a crucial point and not to be ignored. The results included combined observation from all participants. Any differences among the four different participant groups have been noted.

Findings

Before the workshops

On average, recruited participants have 3-4 IoT products in their household. Nearly all participants we spoke to own a smart mobile. Smart thermostats, speakers, watches/fitness tracking devices, and tablets were among the more frequently used products.

Concerns about privacy or sharing of personal information were not priorities for participants prior to the research.

“Fundamentally I have not got a problem with it...I trust the Government.”

– A participant from the 35-54 year old/family group

Benefits of smart features were frequently mentioned, along with other product attributes such as design and general functions. Hardly any negatives were directly linked to the smart features of the products.

Participants appreciate smart features such as connectivity, the ability to find their devices, tracking features on health devices, remote control functions, the convenience provided, and potential cost savings.

“I like the ability to operate all aspects of my home regardless of where I am in the world. The automation is great, which makes my life easier, like heating the house when I am close and turning it off when I leave, or turning the lights on and off when it gets dark, to appear like I am at home.”

– A participant from the aged 35-54 year old/family group

Some participants indicated dissatisfaction, particularly noting the poor integration between various products. Out of 22, there was only one individual who raised concerns about security issues and took proactive measures to address them.

Before the research workshop, participants did not have major concerns about IoT products collecting their personal information.

“Smart devices, being ‘smart’ it is in their nature to be collecting information.”

– A participant from the group aged between 18-34

There was a positive perception around ‘health’ information being collected on smartwatches so they can monitor and track how they are getting on. However, there were some concerns when it came to IoT products, such as connected doorbells, and taking videos without them knowing. When it comes to taking precautions to protect personal information beyond security measures, participant responses were polarised with some taking some action and others doing nothing.

“I do look through how my data is used and deselect any ‘personalised’ advertising data and when I remember I delete voice commands in Amazon that it stores.”

– A participant from the vulnerable group



Smart Guitar...connects to other users worldwide for jamming sessions. On line tutoring available as well as different rhythms and sound effects.

14:28



Smart cleaner. Time saving device which works via Wi-Fi. Easy to set up, removes a lot of dust from whole of house. Can be programmed to with through the night

14:26

Images shared by respondents during the WhatsApp pre-tasks

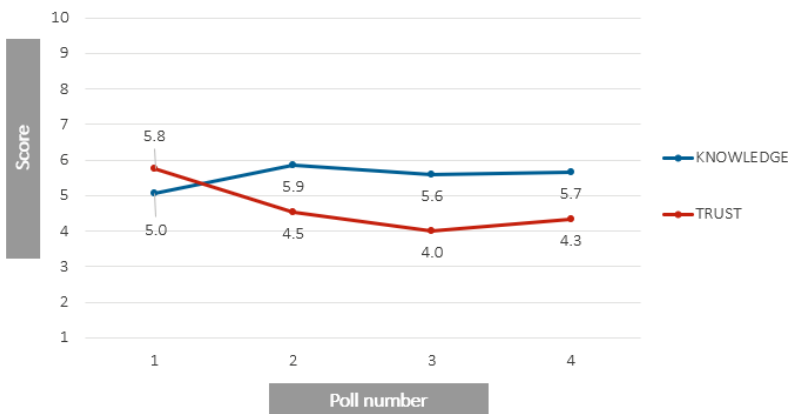
During the workshops

Mapping perception change

From the start of workshop 1 to the end of workshop 2, we conducted 4 polling exercises to measure participants' awareness of how IoT products use personal information and the trust levels in IoT manufacturers. As we progressed through the research, awareness went up slightly, while the trust levels dropped, indicating that as participants learn more about various areas of the research content, they trust IoT products and manufacturers less with their personal information.

Level of Knowledge vs. Trust:

Poll 1 was taken at the beginning of Workshop 1, Poll 2 at the end of Workshop 1, Poll 2 at the beginning of Workshop 2 and Poll 4 at the end of Workshop 2



Difference from Poll 1 (beginning of Workshop 1) to Poll 4 (end of Workshop 2)

Knowledge	Total	Vulnerable	18-34	Middle age/families	55+
Increase # people	13	2	3	3	5
Same # people	2	0	1	1	0
Decrease # people	5	2	1	1	1
Missing # people	2	1	0	1	0

Trust	Total	18-34	Younger	Middle age/families	55+
Increase # people	3	1	0	0	2
Same # people	3	2	0	1	0
Decrease # people	14	1	5	4	4
Missing # people	2	1	0	1	0

Q: How much do you think you know about how technology companies/manufacturers of smart products use your personal information? n=20

Q: How much do you trust technology companies/manufacturers of smart products to keep your information safe and private? n=20

In the final polling exercise, we asked the participants to prioritise different areas of the IoT guidance to manufacturers. The ranking below broadly reflects the conversations participants were having in the breakout groups. It's worth mentioning, that several participants said they found it hard to prioritise as they found all topics of high importance.

"All of those could have been number one in my view."

– A participant from the 55+ group

Overall, the mention of security measures and encryption resonated with most participants, potentially because of their familiarity with the concept from other online services (like WhatsApp) they use regularly.

The ranking exercise had shown that guidance propositions around control over personal information and transparency resonated with participants strongly. Out of this group of propositions, their ability to make decisions about information being shared with third parties received the most votes. It was followed by the proposition about having the option to withdraw consent for their data being collected or shared. We found that these topics produced the most lively discussions in the workshops with participants being engaged and providing many suggestions for improvement of the current state of IoT products.

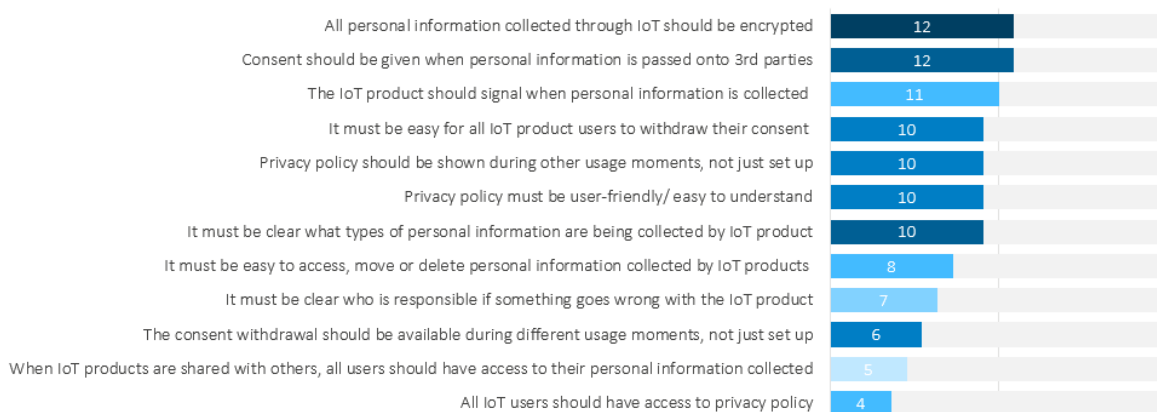
We can clearly see from the final ranking of propositions that the participants value transparency about how IoT products use their information and that this is closely linked to them being able to exercise control over it. Participants struggled to separate the two topics in the discussions and often found that their suggestions for improving consent would also improve the provision of transparency information.

Although participants recognised the importance of being able to exercise their rights, they ranked them lower than the areas of the guidance which focus on transparency and control over their personal information. In their conversations, participants stressed that they like to know their rights are available to them, but they are not very experienced at using them in practice.

The parts of the guidance which would focus on provisions for products with multiple users also ranked lower, reflecting the issues participants had with understanding how some of these provisions would technically work in practice. Similarly, the lack of practical experience in establishing who is responsible for proper functioning of IoT products has potentially meant that participants ranked this guidance proposition to be of lower importance to them.

Guidance topic priority – top 5 rank

(The number of participants (out of 22) selecting the topic in top 5)



Q: In this session, we discussed different areas ICO are looking into. Which areas would you want ICO to prioritise? n=21

Privacy and security when setting up an IoT product

This section describes how participants handle choices about privacy and security when first setting up an IoT product.

Participants valued security features such as encryption, despite not exhibiting security-conscious behaviours.

Encryption was seen as valuable, but not always a primary consideration in purchasing decisions, partly due to limited awareness about which IoT products offer it. Trust in brand reputation and the functionality of the product often takes precedence. Participants assume products are secure when they buy them and that well-known brands will apply best practices to keep their personal information secure.

While participants valued encryption, most participants showed basic or no understanding of how encryption works as a security measure that protects data from unauthorised access.

“If somebody said to me, yeah, you know, this is, security is encrypted, the question is, but what does that actually mean in practice?”

– A participant from the 35-54 year old/family group.

Awareness of encryption may be higher due to recent marketing campaigns of big communication apps such as WhatsApp, a product highlighted by participants for its use of encryption. However, participants were less clear about encryption in other IoT products like TVs or smart home appliances, and therefore did not know whether their IoT products encrypted data. When encryption was explained, the general concept of it seemed to be understood.

Response to the ICO guidance proposition⁵

Proposition 10

Although not all personal information needs to be encrypted, companies should encrypt any information which is classed as ‘special category’ (voice, face scans, heartbeat or gait).

The general sentiment from participants towards this guidance proposition was that it is actionable and realistic. All agreed that there should be differentiated security protections based on the type of information. There was a clear consensus that biometric data (voice, face scans, fingerprints) and health-related information warrant the highest level of protection. These data types are uniquely personal and could lead to significant privacy invasions or identity theft if compromised.

⁵ See Appendix C for full proposition wording

Participants suggested the following to consider:

- **The 18-34-year-old group** emphasised the importance of protecting information that could be used in a discriminatory manner, suggesting a person-specific approach to data protection.
- **The 35-54/ family group** and **vulnerable groups** questioned the need for differentiation, advocating for universal encryption as a simpler and possibly more effective strategy.
- **The 55+ age group** suggested additional protections for products that collect information they consider sensitive, such as sound and/or video.

“Why differentiate? If it truly is just as easy to encrypt everything, so why not just encrypt a whole lot?”

– A participant from the 35-54 year old/ family group

The feedback underscores a strong desire for robust security measures that go beyond encryption. This included two-factor authentication, regular updates and patches to address vulnerabilities as they are discovered, transparency from manufacturers regarding what information is encrypted and the specific encryption standards used or education from manufacturers for participants on safely using IoT products and protecting their personal information.

Participants suggested the following points to consider:

- Encrypting all personal information
- Providing specific encryption standards - the proposition mentions the need for encryption but does not specify the encryption standards or levels required.
- Participants also highlighted the need for clearer information on the security of IoT products to aid purchasing decisions, suggesting having a certification or trust mark that could help consumers identify which IoT products are secure and ensure the privacy of personal information.

Participants appreciated the need for strong passwords but did not always set them.

Overall, while there's an understanding of the importance of security measures like strong passwords, practices differ widely among participants. The frequency of changing passwords varied, with some admitting they don't change passwords as often as they should. Only a few participants mentioned using password managers or system-generated passwords to maintain strong security without having to remember complex passwords.

The youngest group, 18-34-year-olds, were more likely to expect products to be secure and trust well-known brands to have covered security aspects. The vulnerable group was more cautious and stated various

strategies like using multiple email addresses when setting accounts and passwords setting accounts with IoT products (and in general). The vulnerable group also discussed the importance of additional security measures, including two-factor authentication to enhance the security of their IoT products and personal information.

Participants feel overwhelmed by privacy information during setup and don't feel their consent is informed.

In discussions, participants often conflated the experience of giving consent with seeing and understanding privacy information.

They feel privacy information is too long-winded, while also unclear about what information is being collected and why. Many felt manufacturers guard information and don't tell them about all the personal information that they collect, with some participants going as far as saying this was intentional.

Privacy policies are often so extensive and complex that users tend to skim-read or not read them at all, leading to a sense of being overwhelmed by the sheer volume of information. This 'Niagara Falls of information' approach is seen as ineffective. In the 55+ group particularly, they mentioned a habit of not reading and simply rejecting everything they can due to their inability to read and take in all the information presented. The complex technology and legalistic language make the information even more difficult for them to understand.

They also expressed feeling disempowered when manufacturers of IoT products ask them to consent to collect their personal information. Participants find privacy information difficult to understand and difficult to remember, leading to a lack of transparency about what they are consenting to.

There was a definite desire to have a clear understanding of why personal information is being collected and what is happening to it. This was seen as essential when giving consent. Suggested improvements included things such as clear categorisation, the inclusion of visuals, bullet points, collapsable lists and large text. Additionally, a few would welcome further education at the point of purchase, for example retail staff who could talk them through information and consent.

Participants feel the current process for understanding privacy information and giving consent is too limited to account setup. This is especially important as feelings, opinions and situations can change, and people likely won't consider the future when providing initial consent.

Collective consent is necessary in theory but hard to achieve in practice.

Participants thought each user of an IoT product should be able to give consent to share personal information, however, some flagged situations where this was seen as less relevant or impractical. An example of this would be having young children in the house, who may not be of age to give proper consent or the feasibility of gathering consent from all individuals in a household every time a new IoT product is purchased.

Response to ICO guidance proposition:⁶

Proposition 1

Manufacturers should consider moments throughout the product lifecycle where it might be appropriate to show privacy information.

They should consider how to ensure everyone can access privacy information when they need it even if they didn't set up the product.

When referring to this proposition, participants found it difficult to separate the concept of consent from seeing the privacy information. Nevertheless, participants felt it was a step in the right direction, appreciating being asked for privacy information at multiple stages and wanted to add other key moments such as:

1. Information is deleted when a relationship ends.
2. Information is automatically deleted after account closure.
3. Clarity as to what happens to information when an account is deleted/deactivated, including the differences between the two situations.
4. Annual privacy reminder in 'tick list' format. Respondents also wanted to see regular reminders, for example, every 3 months and reminders at key milestones, for example, after a year.

Despite welcoming this guidance proposition, some were unsure how practical it would be. This was particularly the case for products without an interactive display such as light bulbs or smart speakers. There were also concerns that consumers may simply dismiss the reminder of the privacy information, due to busy lifestyles or lack of interest.

Participants suggested the following points to consider:

- First and foremost, the format of the privacy information has to be easily accessible.
- Similarly to the consent proposition, a periodic privacy reminder would be useful.
- Format suggestions included: a tick list, email, manufacturer's website, or the product itself (all being associated with ease of access). Those in the youngest age group also referred to apps, QR codes and the use of video tutorials.
- There was a suggestion by some that the IoT product's service should be paused until the user interacts with the privacy document.

⁶ See Appendix C for full proposition wording

Response to ICO guidance proposition:⁷

Proposition 2

Manufacturers should make it easy for people to understand what their consent is for, why it is required and how to change it at a later date.

Manufacturers should consider moments throughout the lifecycle of the IoT product where people who use it may need to give or change their consent.

“A guest function or something that if it registers that there's somebody else in the house...you can just turn it off and say you can't gather any of that information for the rest of the evening and that would be enough. Telling it you don't want it on just now, it should just be a button to be like you're no longer listening or whatever.”

– A participant from the 18-34 year old age group

Participants liked the explanatory aspect of the proposition and felt this was a step in the right direction when it came to removing ambiguity regarding why and what personal information is captured. This would help provide them with much-needed transparency when it comes to the collection of personal information by IoT products. The vulnerable group were the most positive regarding this proposition. The younger group made suggestions for how to avoid situations with non-household members having their information collected and having to potentially ask them for consent.

“It would be good for apps and devices to have little reminders to just remind you of the T's and C's and remind you again if you want to opt in or opt out. Because obviously we've all got really busy lives and that some of us aren't as proactive as others. And I probably wouldn't go back, but if I was reminded it might make me look at it.”

– A participant from the 35-54 year old / family group

Participants suggested the following points to consider:

Participants felt consent moments should reflect the dynamic nature of their lives, for example when someone comes of age or becomes ill. Solutions included:

- A 'tick list' of choices at key moments such as setup when a new account is added, or when a security update is made.
- A regular recapturing of consent, at intervals of around 3 months to a year.

⁷ See Appendix C for full proposition wording

Participants had differing opinions on whether personal information should be used for profiling, but all agreed they lacked information.

Participants acknowledged that most consumers would be surprised by the amount of information that companies have collected about them, indicating a need for better awareness and being told in advance about data practices from manufacturers. Participants had mixed perceptions towards data collection for profiling and personalisation:

- Some participants were not entirely comfortable with profiling practices, but they accepted them as a part of modern life, focusing instead on the potential benefits or simply resigning themselves to the inevitability of being profiled. This sentiment is more common among the vulnerable group.
- Some participants saw the value in personalisation, appreciating the convenience and relevance of tailored advertisements and recommendations.

"I think it's quite useful [...] I go to see quite a lot of concerts and bands and [...] you start getting all these adverts about similar sorts of bands that you might like to go and see. [...] some of it is actually quite smart and useful."

– A participant from the 35-54 year old/family group

A significant number of participants expressed concern about the implications of their information being used for personalisation. The concerns included:

- **Lack of transparency and control:** Frustration with the complexity and obscurity of privacy information related to data collection, leads to a desire for clearer information and more straightforward ways to opt out or control how personal information is used.
- **Privacy invasion:** Personal information is used in ways they have not explicitly consented to, leading to a feeling that their private lives are being intrusively monitored and exploited for commercial gain.
- **Data security:** Shared information could be mishandled, leading to potential breaches where sensitive information might be accessed by unauthorised parties.
- **Misuse of information:** Personal information could be used for purposes other than what was intended, including being sold to third parties, leading to unwanted contact or scams.
- **Manipulation and behavioural influence:** Personal information used for targeting can lead to manipulation of choices and behaviours, potentially impacting autonomy, and freedom of choice.
- **Over-personalisation:** Algorithms are shaping their online environment to such an extent that it creates a "filter bubble," potentially limiting exposure to diverse information and viewpoints.

Some participants were aware that although they may not be able to completely avoid being profiled, they know they can take steps to reduce the impact of profiling:

- **Opting out/consent management:** they are cautious about giving consent when signing up for new services or buying IoT products, often looking for ways to opt out of data sharing at the point of purchase or setup.
- **Adjusting privacy settings:** they take time to adjust privacy settings on their products to limit the amount of information that can be collected about them.
- **Information withholding:** they avoid providing real names, ages, or other personal details when setting up profiles on products or online services to keep their true identities obscured – this view was especially prevalent in the vulnerable group.
- **Educating themselves:** they try to educate themselves using the privacy policies, though they find this information often complex and not user-friendly.

Regardless of how participants feel about profiling, there is a clear call for greater transparency, simpler controls, and assurances that personal information is used responsibly and ethically.

Response to the ICO guidance proposition:⁸

Proposition 6

Manufacturers wanting to share or sell information for advertising must ask people for their consent. They should provide granular options for what type of personal information from an IoT product can be shared for advertising.

Manufacturers must give people details about a) the categories of information they hold (for example, contact details, interests or special category information - political views and religion), and b) the source of their information (for example, the organisation it came from).

There is a consensus among all groups that there should be more granular controls over the personal information gathered by IoT products for advertising purposes. Consumers should be able to control what information is shared for advertising purposes at the point of initial setup and have the ability to adjust these preferences easily at any time.

The types of information participants are most concerned about include health metrics (for example heart rate, sleep patterns from fitness trackers), location data, political views, religious beliefs, and financial information. Participants indicated that IoT products collecting these types of personal information should clearly explain when asking for consent how they use them in their profiling practices.

⁸ See Appendix C for full proposition wording

Participants suggested the following points to consider:

- Easier ways to opt-out or control data-sharing preferences. Despite a requirement for opt-in rather than opt-out already existing in the law, participants didn't seem to be aware of it and felt like they wanted to have it available from manufacturers. This feeling was especially prominent among the 55+ group.
- Periodic reminders or check-ins would help them review and adjust their consent settings.
- Automatic deletion of the information stored after a certain period.

“And why is it always us that has to unsubscribe?”

– A participant from the 55+ age group

“Have a cut-off point where they should just not keep it. What is the relevance of them keeping it?”

– A participant from the 18-34 age group

Considering privacy while using an IoT product

In this section, we will focus on guidance areas that are linked to the stage where an IoT product is in use.

Participants think IoT products should actively signal when collecting personal information.

Throughout the workshops participants voiced concerns about not being aware of the personal information IoT products collect. Participants were asked to consider if a signal would be appropriate to indicate when an IoT product collects personal information. Broadly they agreed that this was important but had reservations about how invasive signalling might be.

Response to the ICO guidance proposition:⁹

Proposition 4

It should be obvious when an IoT product is collecting personal information, especially when the product is not in direct use.

Participants resolutely agreed that it was an incredibly important requirement, as signalling would help boost transparency which was seen as a positive. Many would welcome knowing when their products were capturing information, and they felt this feature would help keep them 'in the loop', for example, knowing when a smart speaker is actively recording. However, some had reservations regarding the effect of being constantly aware of a product recording.

Some questioned practicalities linked to multi-user experience. For the product signalling when having visitors, they might not want to check for signal mid-conversation, and they would not take friends through a privacy policy when they arrive at their house.

Sound or light were regarded as the most appropriate forms of signalling, with some participants desiring both at the same time. Some were concerned with intrusiveness, such as speakers in bedrooms at night, with the solution being the option to have a 'no notification' period. There should be considerations for those with impairments to suit their preferences.

⁹ See Appendix C for full proposition wording

Participants suggested the following points to consider:

- Participants wanted the ability to retract information once they were made aware a product was collecting information (especially among the 55+ group).
- They also wanted clarity as to why a device was recording. For example, the vulnerable group appreciated that some smart speakers make a sound when recording but few understood why exactly it was recording.
- In the 35-54 year old / family group, there were comments made regarding acknowledgement from a device when it is collecting information from a different person, for example, if someone new entered the room.

Participants had not tried to withdraw their consent from IoT products.

Very few participants had a direct experience of withdrawing consent from an IoT product. Some participants provided examples of adjusting consent or permissions on general apps and websites, for example deleting or not accepting cookies or adjusting settings on apps.

Response to the ICO guidance proposition:¹⁰

Proposition 3

Manufacturers must make it easy for everyone who gives consent for an IoT device to use their personal information to withdraw their consent at any time.

The proposition was well received, as participants feel that the collection of their personal information is often excessive and unnecessary. They also cited previous experiences where participants felt forced to consent to things they did not necessarily want to do for fear of not being able to use the product.

While participants agreed in principle this option should be available for everyone using the product, they felt it might be impractical and appreciated it would be difficult for manufacturers to implement. As such, the vulnerable group thought that the ICO should be lenient when considering enforcement in this area.

Participants suggested the following points to consider:

- Among the 55+ group, they wanted manufacturers to make it clear what, if any, are the consequences of withdrawing consent.

¹⁰ See Appendix C for full proposition wording

Few participants had tried to access their personal information from products and were unsure of what they would do with it if they could.

Many said they lacked confidence in their ability to access personal information from IoT products. They also felt unsure about what they would do with the information if they were to access it, some would do it out of curiosity or to ensure privacy and security. Only a handful had attempted to access their personal information in the past.

Despite their limited experience, there was a mention of the need for regulatory bodies or standards to improve the situation regarding the management of personal information on IoT products. Specifically, the idea of having some sort of certification or trust mark that could help participants identify which IoT products are secure and respect privacy was brought up.

Response to the ICO guidance proposition:¹¹

Proposition 7

IoT manufacturers must allow everyone who shares personal information with an IoT product, regardless of whether they are the registered owner or not, to exercise their rights.

There's a strong endorsement across all groups for this proposition, however, participants had concerns about the practicalities of this proposition. Similarly, to providing consent, participants were unsure how this can be enabled when multiple users are involved. Participants called out the social awkwardness of enforcing these rights in personal settings and the technical challenges of implementing systems that would allow non-owners to exercise their rights effectively.

"You have to accept that you're on my ring doorbell when you come into my house because you're going to be on my ring doorbell."

– A participant from the vulnerable group.

Participants suggested the following points to consider:

- Specific mechanisms for non-owners to exercise their rights, although they acknowledged this may be hard to achieve.
- Handling of personal information after death (outside of the ICO's remit).

¹¹ See Appendix C for full proposition wording

Participants generally felt comfortable sharing information within households but recognised that might not be the case for all.

In most situations, information from IoT products was controlled and accessed mainly by the account holder, this was not seen to be an issue due to trust within the family.

The logistics of applying individual accounts and profiles in a household were questioned, particularly as there is often just a sole account manager in charge of an IoT product.

However, a few in the 35-54 year old / family group did refer to situations in which having multiple people's information controlled by one account manager might be a potential risk, for example, coercive control in relationships (for example to see when somebody is coming in and out of the house).

Other participants felt the type of IoT product may affect levels of comfort in terms of sharing personal information within households, for example IoT products that collect audio. They would not want other household members to have access to conversations that took place when they were not present.

Their main feeling about sharing information was linked back to a lack of knowledge of what type of information is being collected. Participants said that they can only really act if they know what information an IoT product is collecting.

Participants agreed that when it comes to IoT products that collect information from multiple users, guidance is needed to clarify ambiguity, both in terms of who should access the information and what their information rights are.

Response to the ICO guidance proposition:¹²

Proposition 5

Manufacturers should provide flexible settings for individuals to share different levels of personal information with others who use the IoT product.

Participants (especially among the vulnerable group) were able to come up with various situations in which having a user with more control than others is desirable, for example for cost control (heating), safety and protection against crime.

Participants also questioned the meaning of the word "flexible" and what that would entail.

Participants suggested the following points to consider:

- Having a tiered hierarchy of control where an account holder has the greatest level of access and privileges while others only have some access/privileges.

¹² See Appendix C for full proposition wording

Participants were less concerned about information sharing between IoT products and were not aware of what to do when things go wrong with multiple products.

Nobody had first-hand experience of issues with personal information being shared across multiple IoT products in their household.

Some participants were aware that products share information with third parties and why they do this. However, they reported greater levels of concern and opposition to personal information being shared for advertising, as opposed to functionality.

There was low awareness of what to do or who to contact when something goes wrong. It was clear participants had experience with IoT products not working properly and often felt limited in their ability to fix them. It was unclear how many of these issues would have been caused by problems with information sharing between products.

When faced with an issue, participants tried various methods such as turning the products off and on, resetting Wi-Fi, or reinstalling software. Despite this, feelings of frustration and difficulty were commonly reported. They try to fix things themselves first, as they feel that the manufacturer's customer services are often unresponsive. Although knowing who is accountable for functioning of the product would be beneficial, particularly when attempting to identify which product is causing the issue, the primary concern for participants here is troubleshooting guidance that would allow them to run diagnostics and solve the issue themselves.

Nevertheless, participants wanted more accountability from manufacturers. Part of this means accepting responsibility for faults, and part of this also entails providing a more comprehensive level of assistance. This assistance can either come from a customer service department or it can be built into the products themselves.

Response to the ICO guidance proposition:¹³

Proposition 9

Manufacturers must provide clear information about all the partners and suppliers who have access to or control over people's personal information. They should also make it clear what type of information they hold.

The inclusion of the word "must" within the proposition was well-received given the fact that it allowed for less ambiguity.

While participants could see how it was important, not all were convinced they would actively go through the effort of finding this information out. This type of information would be something they would like to be

¹³ See Appendix C for full proposition wording

able to have access to but may not necessarily want to know. Some expressed concern that knowing this, particularly if it was a large number of third parties, would be overwhelming.

In terms of when participants would like to see this information, there were some suggestions that this could follow a similar process to the key moments in a product lifecycle similar to showing privacy information in Proposition 1.

Participants suggested the following points to consider:

- **The vulnerable group** picked up the difference between the terms “access” and “control” used in the proposition. The feeling was that these could have drastically different implications, and therefore would need to be more clearly explained.
- **The 55+ group** suggested there should be something in the proposition about the accessibility of the language given that many people who rely on this type of technology in their day-to-day life may be disabled.

“Control of your data sounds terrifying to me.”

– A participant from the vulnerable group

Protecting your privacy when disposing of IoT products

In this section, we will explore areas linked to the end of the product lifecycle, when selling on or disposing of an IoT product.

Data portability is seen as valuable, but few have tried it.

There is an understanding that technology is advancing, and data portability should be possible with the right security and user-friendly approaches. Some of the hypothetical examples of when data portability might be useful were upgrading or switching IoT products, product failure or replacement.

In terms of moving personal information, changing mobiles was used as the main example, as not many had tried to move their information from one IoT product, as defined in our research, to another.

Participants are sceptical that their personal information is actually deleted.

Only a few participants tried to delete their personal information from IoT products. Some expressed knowledge or willingness to attempt, often suggesting a factory reset as a solution, but there remains scepticism regarding its effectiveness in completely erasing personal information. Some debated whether manufacturers were retaining their information even after the supposed deletion.

"You can reset it to factory settings. But do we know really that that works?"

– A participant from the 55+ age group

A few, mainly among the vulnerable or older groups, mentioned avoiding the risk of sharing their personal information by not selling or giving away their IoT product (such as Fitbit).

"I would have to get advice because I would not know what to do. I would rather destroy the product."

– A participant from the vulnerable group

One participant had a real-life experience accessing somebody else's information when he sold his car:

"I had OnStar with my old car, which you could use to check your car and do all sorts of various bits and pieces with. When I sold my car back to Vauxhall, I told them that [about OnStar]. But for the remaining two years of my OnStar subscription, they never even repeated phone calls. They never stopped me from accessing the information, so I could see where the new owner was, and I could unlock the car."

– A participant from the 35-54 year old / family group

Whilst using IoT products, the majority would like to be assured that their rights over their personal information are available to them if they want to exercise them.

Response to the ICO guidance proposition:¹⁴

Proposition 8

IoT manufacturers should ensure that they have easy ways for people to request their information from IoT products to be moved to a different company.

Similar to being able to access their information, the idea of being able to move information is welcomed but participants acknowledged that this right is only useful if they can understand what information IoT products hold.

Younger participants seemed to believe it was actionable and realistic, especially as they value the convenience and continuity of their digital experiences across IoT products.

Some participants (mainly among older and vulnerable) expressed scepticism about the feasibility of implementation, particularly when considering different brands with potentially incompatible systems.

If moving personal information is required, the preference of the majority is for a simple and automated process that facilitates an easy and secure transfer of information allowing them to select what types of information to transfer with minimal effort.

Participants suggested the following points to consider:

- The desire for clear and mandatory language ("must" instead of "should") regarding the ability to delete personal information.
- Users should have the ability to choose what information is moved.
- Assurance that once personal information is transferred, it should be securely deleted from the old IoT product to prevent unauthorized access or misuse.

"Perhaps whilst they're moving information, I can have a say in exactly what is moved. For example, I might want my steps to be moved, but maybe not some of my other fitness history."

– A participant in the 18-34 year old group

¹⁴ See Appendix C for full proposition wording

"If you're swapping from Apple to Samsung or whatever, all your data from your Apple phone ...is being deleted whenever you have successfully transferred it over."

– A participant in the 18-34 year old group

Conclusion

The participant deliberations provided in-depth insights into what the informed public find acceptable and what goes beyond their expectations when it comes to IoT products using their personal information. The research extracted rich perspectives on how people use their IoT products, what encourages them to embed them in their lives and what discourages them from using all of their smart features.

The recommendations articulate participants' conditions for trustworthiness and expectations for how IoT manufacturers should protect personal information. They provide a clear list of suggestions for the ICO to consider in the policy development process for the upcoming guidance.

This research emphasizes the importance of continued public engagement to ensure that the future developments in IoT align with the values and expectations of the people using these technologies.

Appendices

Appendix A - Definition of the Internet of Things

We showed the following definition of Internet of Things to the participants in the first workshop:

The Internet of Things describes the network of physical objects ('things') that can connect and share information with other things and systems over the Internet. These 'things' can sense, respond to, or interact with the external environment, powered by a large range of technologies (such as biometric or environmental sensors, artificial intelligence). IoT products process large amounts of often highly personal information about people who use them and people who are exposed to them.

IoT products can be used in many settings. For example:

1. People monitoring their wellbeing,
2. People managing their homes,
3. Organisations monitoring their employees,
4. Hospitals treating patients,
5. Schools educating children,
6. Factories managing effective production of products,
7. Cities to measure traffic and how busy certain areas are.

For this research, we are only interested in the use of IoT products which would fall under points 1) people monitoring their wellbeing and 2). people managing their homes and setting up entertainment.

As consumers, people are most likely to come across IoT products like smartwatches, fitness trackers, smart kettles, thermostats, doorbells, smart TVs, and smart speakers.

IoT products process large amounts of often highly personal information about people who use them and people who are exposed to them.

Appendix B - Transcripts of Which? videos shown to participants in workshop 1

Area 1 (Making choices about personal information):

SECURITY
TRANSPARENCY & CONSENT
PROFILING
DATA SHARING


MAKING CHOICES ABOUT PERSONAL INFORMATION

Stimuli provided to respondents (presented as a video):

Imagine you get a smart speaker for Christmas and you set it up at home, when you ask it a question or ask it to play you some music, you are interacting with not just a single company but a whole host of different providers.

Now some of these will be providing you with important services, some will want your information for advertising.

You are asked to give your consent in a flurry of excitement to set up a new product it is easy to just click accept, but do we really understand what we are signing up to and if this device is going to be used by other people in your home, can we really say yes to everybody all at once?



INDIVIDUAL RIGHTS
ACCOUNTABILITY

Privacy

How does Smart Speaker receive the amount of data sent to the Cloud?

What happens when I speak to Smart Speaker?

What about "wake words"?

How do my voice recordings and data transfer to other Smart Speakers?

How do I know when Smart Speakers are sending data to the cloud?

Can I turn off the microphones on Smart Speakers?

Is Smart Speaker recording all my conversations?

Can I review, manage and delete my voice recordings?




Area 2 (Making product features and adverts specific to you):

SECURITY
TRANSPARENCY & CONSENT
PROFILING
DATA SHARING


Making adverts specific to you

Stimuli provided to respondents (presented as a video):




Think about your household and who lives in it, no one is exactly the same, a smart TV for example can be used by parents, children and maybe even grandparents, all with different preferences on what they would like to watch.

Some smart products let you set up profiles to tailor recommendations to your needs, this means a more personalised experience when it comes to films and TV shows to watch. The trade off is you are sharing more information about what you and your family like.

Think to yourself, if this was used for marketing and advertising purposes, how would you feel about that?



INDIVIDUAL RIGHTS
ACCOUNTABILITY

Area 3 (Sharing information within your household):

SECURITY | TRANSPARENCY & CONSENT | PROFILING | **DATA SHARING**

Sharing information within your household

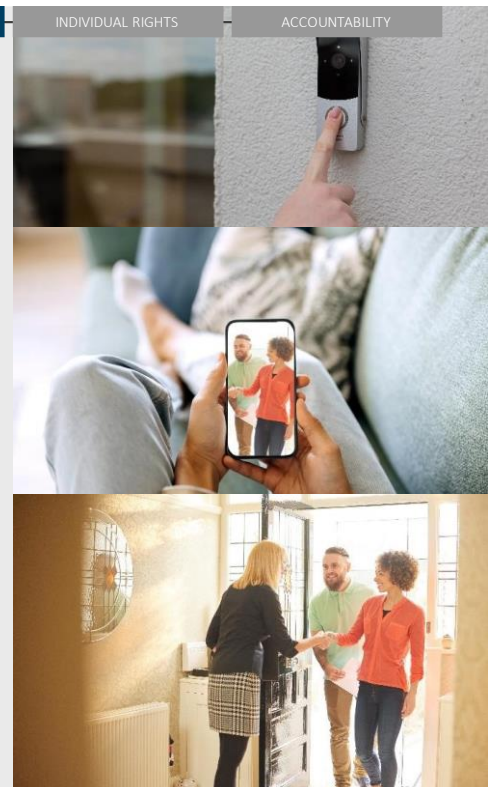
Stimuli provided to respondents (presented as a video):

Smart doorbells are useful gadgets to manage the comings and goings of your front door but what if you're a night owl and your housemate is an earlier riser, you won't necessarily want them knowing when you arrive home from a night out.

Individual accounts and profiles can help personalise the experience with smart gadgets but what if they are not available?

Would you worry about sharing more information than you wanted with other members of the household?

Which?



Area 4 (Your rights over your personal information):

SECURITY | TRANSPARENCY & CONSENT | PROFILING | **DATA SHARING**

Your rights over your personal information

Stimuli provided to respondents (presented as a video):

There may come a time when you want to move on from a smart product, either because it is faulty and you bought a new one or you want to pass or sell it on to a new owner.


We have often found problems in our testing with the effective removal of personal information from devices, sometimes it is near impossible.

You don't want the new owner of your fitness tracker for example knowing more about you than they should and also when you set up your new device, you want to take all your important and fitness information with you, and not, this is the most important thing, need an engineering degree to do so.


Which?



Area 5 (What happens when things go wrong with more than one IoT product):

SECURITY	TRANSPARENCY & CONSENT	PROFILING	DATA SHARING	INDIVIDUAL RIGHTS	ACCOUNTABILITY
<h3>What happens when things go wrong with more than one IoT product?</h3> <p>Stimuli provided to respondents (presented as a video):</p> <p>Smart products are meant to be, well smart. Take a smart thermostat for example, you can set the heating with a tap on your phone or even your voice if you have it connected to a smart speaker.</p> <p>However, we then rely on all these companies working together to ensure that everything functions properly. You don't want your heating clonking out in the middle of winter because your smart thermostat no longer likes your smart speaker.</p> <p>When your products are not doing their jobs, what would you do?</p>					
<h1>Which?</h1>					

Area 6 (Security of IoT products):

SECURITY	TRANSPARENCY & CONSENT	PROFILING	DATA SHARING	INDIVIDUAL RIGHTS	ACCOUNTABILITY
<h3>Security of IoT products</h3> <p>Stimuli provided to respondents (presented as a video):</p> <p>All too often in Which? testing we expose smart products that don't effectively protect you from hackers, including something as sensitive as a baby monitor. Information on you can be intercepted by cybercriminals and can be used as part of scams or fraud or the device itself can be used to spy on you.</p> <p>Companies can protect smart products by using various measures like encrypting your information so no one can see it, sadly though not all manufacturers elect to do so.</p> <p>When you're shopping for smart products have you ever considered whether it is secure?</p>					
<h1>Which?</h1>					

Appendix C - ICO guidance propositions

The guidance propositions were drafted by the ICO. We showed these materials as stimuli to participants ahead of the workshop 2. The stimulus materials were referred to again during the workshop 2.

1. Making choices about personal information

Often the person who first sets up an IoT product will see privacy information and make privacy choices on behalf of the household.



a) Manufacturers should consider moments throughout the product lifecycle where it might be appropriate to show privacy information:

1. During set-up
2. When the product collects personal information about a new person or a new account is added
3. During a security or product update which changes how personal information is processed

b) They should consider how to ensure everyone can access privacy information when they need it even if they didn't set up the product:

1. Make privacy information visible on the app store so everyone can access it
2. If there is a companion app, make sure privacy information is easy to find for everyone who has an account
3. Provide a way to find privacy information directly through the product's interface rather than through a companion app

2. Making choices about personal information

In many instances, people will need to give their consent for an IoT product to use their personal information. Sometimes this might mean giving consent on behalf of the household or another family member.

a) Manufacturers should make it easy for people to understand what their consent is for, why it is required and how to change it at a later date.

- They must present these choices in a way that is easy to use and does not unfairly influence someone to make one choice over another.
- Manufacturers must make it easy to withdraw consent if someone changes their mind and or wants to change specific permissions around how the IoT product uses personal information.

b) Manufacturers should consider moments throughout the lifecycle of the IoT product where people who use it may need to give/ change their consent:

1. During set-up
2. If the IoT product collects personal information about a new person or when a new account is added
3. If a security or product update changes how personal information is processed
4. If someone deletes an account or wants to withdraw their consent
5. If a parent/ guardian needs to give or change consent on behalf of a child
6. If a young person becomes old enough to give consent for themselves (above 13)

3. Making choices about personal information

Manufacturers must make it easy for everyone who gives consent for an IoT product to use their personal information to withdraw their consent at any time.

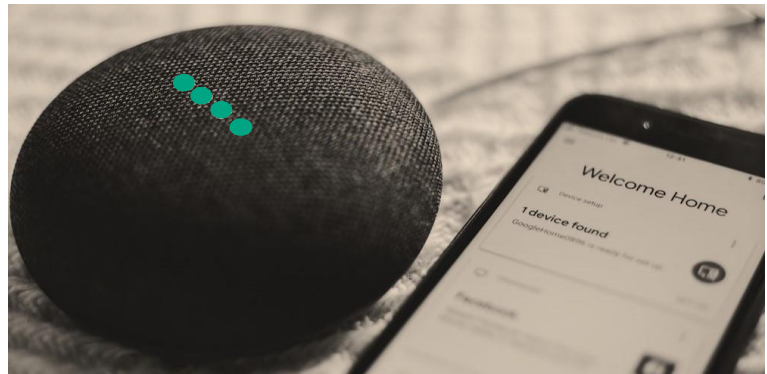
- It should not matter if they are not the registered owner of the product and do not have access to the companion app.
- For example, someone who consents to sharing personal information with a smart speaker at someone else's house must be able to withdraw consent even though they aren't the registered owner of the IoT product and do not have access to the app that controls it.



4. Letting you know when IoT products collect personal information

It should be obvious when an IoT product is collecting personal information, especially when the product is not in direct use.

- Manufacturers must provide visual or audio signals to indicate to those around when the product is currently collecting personal information.
- For example, a smart speaker may show a green light when it is recording and analysing sounds or voices and a red light when it is not.



5. Sharing information within your household



Manufacturers should provide flexible settings for individuals to share different levels of personal information with others who use the IoT product.

- Some IoT products, like doorbells, smart speakers, thermostats or security cameras, can be used by multiple people.
- Individuals who use the product may have different levels of comfort in sharing their personal information depending on the nature of their relationship.

Produced by Impact Research Ltd in strict confidence

5 **IMPACT**

6. Making product features and adverts specific to you

Manufacturers can share personal information collected from an IoT product with other organisations. But it has to be fair, they can't share unnecessary information or anything people wouldn't expect to be shared.

a) Manufacturers wanting to share/ sell information for advertising must ask people for their consent. They should provide granular options for what type of personal information from an IoT product can be shared for advertising.

If an IoT product itself can show advertising, for example in the companion app or on a screen (like a smart TV), manufacturers should provide granular options for whether these ads can be targeted based on the information from the IoT product.

b) Manufacturers must give people details about:

- **The categories of information they hold (for example, contact details, interests or special category information-political views & religion)**
- **The source of their information (for example, the organisation it came from)**

Manufacturers can get additional information about people from other sources and combine these to create profiles of interests and behaviours based on their use of an IoT product. This can help them target their marketing messages to the groups of people they want to reach.

For example, information about poor sleep from a fitness tracker matched with information about recent purchases of nappies could result in an ad for a baby monitor targeted at a sleep-deprived parent.

Produced by Impact Research Ltd in strict confidence

6 **IMPACT**

7. Your rights over your personal information

The UK GDPR gives people various rights to their personal information.

These rights include:

- People have the **right to be informed** about the collection and use of their personal information by the IoT manufacturer.
- People have the **right of access** to their personal information from the IoT product and should be able to request a copy.
- People have the **right to rectification** to request that inaccurate information is rectified, or that incomplete information is completed.
- People have the **right to erasure** and have their personal information deleted from the IoT manufacturer's systems.

IoT manufacturers must allow everyone who shares personal information with an IoT product, regardless of whether they are the registered owner or not, to exercise their rights.

- IoT manufacturers should ensure that additional people who use the product can identify themselves to the company if they choose to exercise their rights.
- Manufacturers should take care to comply with people's requests but not infringe on the information rights of other people using the IoT product.
- Where manufacturers provide settings within an IoT product or its app to exercise people's rights, they should make sure this option is available to all people who interact with the product, not just the person setting up the account.
- This would mean that the option to delete personal information or to access it through the product's settings is available to all who would like to make use of these features.

Produced by Impact Research Ltd in strict confidence

7

IMPACT

8. Your rights over your personal information

The UK GDPR also gives people the right to data portability—the right to move, copy or transfer personal information easily from one IoT product to another, safely and securely.

IoT manufacturers should ensure that they have easy ways for people to request their information from IoT products to be moved to a different company.

- People are allowed to move the information they give their IoT product, like their name, email address, age or username.
- They can also ask for information from their IoT product about for example, their exercises, heart rate readings or settings for automatic lights.
- This could be through a setting within a product's companion app, directly on the product or on their website.
- Manufacturers should also make sure they can receive and integrate information from IoT products from other brands into their own products.



Produced by Impact Research Ltd in strict confidence

8

IMPACT

9. Your rights over your personal information

Manufacturers must provide clear information about all the partners and suppliers who have access to or control over people's personal information. They should also make it clear what type of information they hold.

- Someone needs to be responsible for the personal information IoT products use. The law requires IoT manufacturers or their partners who help make IoT products to take this responsibility.
- Sometimes, there can be hundreds of companies involved in creating an IoT product and using people's personal information. This makes it difficult for people to know who is responsible for ensuring their personal information is safe, who to go to when something goes wrong or if they want to exercise their information rights.



Produced by Impact Research Ltd in strict confidence

9 **IMPACT**

10. Security of IoT products



- Manufacturers and other partners and suppliers involved in producing an IoT product must apply appropriate security measures when they use people's personal information.
- Encryption is one of the techniques which can be used to enhance the security of an IoT product and prevent unauthorised or unlawful use of people's information. Encryption is a mathematical function using a secret value—the key—which encodes data so that only users with access to that key can read the information.

Although not all personal information needs to be encrypted, companies should encrypt any information which is classed as 'special category' (voice, face scans, heartbeat or gait).

Produced by Impact Research Ltd in strict confidence

10 **IMPACT**

About Impact

Impact Research is a full-service market research consultancy based in Walton-On-Thames, Surrey founded in 2010 by Darryl Swift and Dr David Pearmain. While Impact initially focused on consumer and utility research, 2017 saw the establishment of the Services Team. 2017 was also the year Impact achieved its ISO 20252 accreditation. This accreditation has been renewed annually since then.

Since its establishment in 2010, Impact has been at the forefront of providing comprehensive market research solutions, blending quantitative and qualitative methodologies to deliver actionable insights. With a dedicated team, Impact has earned a reputation for excellence and innovation in the field of market research.

Over the years, Impact has successfully executed projects for clients in various sectors, including food and drink, building materials, local authorities, gas, electricity, water, and government agencies. Impact's track record of delivering high-quality research and actionable recommendations has established us as a trusted partner for organisations seeking to make informed decisions.

In this report, Impact delves into the realm of IoT products, leveraging their expertise and experience to provide valuable insights and recommendations for the Information Commissioner's Office.