Which?
2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Consultation Response

Which? response to the Information Commissioner's Office consultation on Draft Guidance for Consumer IoT products and services.[1]

Submission date: 05/09/2025

Summary

Which? welcomes this opportunity to respond to the ICO's proposal to introduce clear guidance[2] to Consumer IoT vendors on how to adhere to data protection regulation, requirements and best practices and the ICO's draft impact assessment.[3]

Our research has consistently demonstrated a repeated and wholesale absence of good data protection processes and privacy-enhancing approaches in consumer IoT, with most products we tested scoring less than 50% on our privacy framework.[4]

Overall, we welcome the ICO's draft guidance for Consumer IoT products and services. We have called for the introduction of such a regulatory initiative for many years, and we feel that it will be a vital step towards improving the inconsistent and often diluted privacy protection measures currently experienced across the Consumer IoT market, such as smart washing machines that request a user's data of birth and access to the users' phone contact list.[5]

---

[1] ICO (2025), *ICO consultation on draft guidance on consumer Internet of Things products and services*. Available at: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2025/06/ico-consultation-on-draft-guidance-on-consumer-iot/
[2] ICO (2025), *Draft Guidance for consumer Internet of Things products and services.* Available at: https://ico.org.uk/media2/2ptpdy3u/guidance-for-consumer-internet-of-things-products-and-services-all-0-0-22.pdf
[3] ICO (2025), *Consumer Internet of Things - draft impact assessment*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/impact-and-evaluation/impact-assessment/consumer-internet-of-things-draft-impact-assessment-june-2025/
[4] Which? (2024), *Smart device brands must put privacy over profits.* Available at: https://www.which.co.uk/news/article/smart-device-brands-must-put-privacy-over-profits-at8Vq4t3VCn9
[5] 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

Over the past two and a half years our Consumer Insight Tracker (a monthly poll weighted to be demographically representative of the national population[6]) has consistently shown that the majority of consumers (between 60-65%) are worried about how data about them is collected and used by businesses.[7]

In our response to the ICO's draft guidance, we argue that in several areas further detail or further commitments are needed to ensure that organisations that process data through consumer IoT have clarity on how to comply with their data protection responsibilities. In particular:

1) The draft guidance must be **clarified** to address the definition of harms (including psychological harm).
2) The draft guidance must be **strengthened** to address inadequacies in the following areas: exemptions of tablets, smartphones, and consumer connected vehicles; permissions and excessive requests for data not essential for functionality; consent journeys from the app download stage onwards (including the experiences of vulnerable users); consumer agency and the ongoing need for ICO enforcement; and data portability.
3) The draft guidance must be **joined-up** for coherence across the legislative and regulatory landscape, in particular: privacy and the consumer rights legislation; online advertising and legitimate interests; location data and UK GDPR; and PSTI and PECR regulations.
4) The draft guidance must be **expanded** to consider ICO engagement with standards development; and to include plans for market investigations, monitoring and robust enforcement by the ICO.

If ICO expects the Consumer IoT industry to improve practices to align with the guidance, then there must be a clear statement of what will happen if this expectation is not met.

We recommend that the ICO commits to a review of the impact of the guidance to check how manufacturers are adhering to their responsibilities under data protection legislation. This could involve setting a strong threshold for harm reduction within a 1-year timeframe, otherwise the regulator would consider deeper market intervention measures.

Without this, companies may continue to underinvest in data protection and privacy measures, and so consumers will continue to be exposed to harms.

---

[6] Which? (2024). *About the Consumer Insight tracker.* Available at: https://www.which.co.uk/policy-and-insight/article/about-the-consumer-insight-tracker-asxTG8k9XrQW

[7] The survey question is: 'How worried are you, if at all, about how data about you is collected and used by businesses? Very worried, Fairly worried, Not very worried, Not at all worried, Not applicable, Don't know.' The proportion of consumers worried is calculated by adding the proportion of respondents that are Very worried or Fairly worried. Which? (2024), *Consumer worries dashboard.* Available at: https://www.which.co.uk/policy-and-insight/article/consumer-worries-dashboard-akJMn5c4FKMv

The ICO's draft impact assessment notes a focus on growth in digital industries. We argue that consumer protection is vital for economic growth[8] and supports innovation and investment.[9] If trust and consumer confidence increase as a result of data privacy compliance, so does the use of Consumer IoT products.

Full response

Overall, we welcome the ICO's draft Guidance for Consumer IoT products and services. We have called for the introduction of such a regulatory initiative for many years, and we feel that it will be a vital step towards improving the inconsistent and often diluted privacy protection measures currently experienced across the Consumer IoT market, such as smart washing machines that request a user's data of birth and access to the users' phone contact list.[10]

We also welcome the presentation, accessibility and clarity of the draft guidance. We have seen with the recent introduction of the Product Security and Telecommunication Infrastructure (hereafter PSTI) Act 2022 regulations[11] how the absence of clear guidance from the regulator causes real problems with market engagement and adherence.[12] So, we support efforts to take a more logical and useful approach here.

However there are a number of areas to improve the draft guidance and provide even greater clarity to the market, and these are indicated below. Most importantly, we are concerned at the lack of a clear plan on how market adherence to the guidance (and so data protection obligations) will be monitored and enforced.

Our research has consistently demonstrated a repeated and wholesale absence of good data protection processes and privacy-enhancing approaches in consumer IoT, with most products we tested scoring less than 50% on our privacy framework.[13] Therefore, we feel the

---

[8] Which? (2022), *Consumer policy for economic growth*. Available at: https://www.which.co.uk/policy-and-insight/article/consumer-policy-for-economic-growth-atjpZ9s9kQb6

[9] Which? (2022), *Consumer protections and economic growth*. Available at: https://www.which.co.uk/policy-and-insight/article/consumer-protections-and-economic-growth-adyma5R8MF2I

[10] 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

[11] DSIT (2023), *The UK Product Security and Telecommunications Infrastructure (Product Security) regime*. Available at: https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime

[12] Which? (2024), *How long will your smart tech last? Big brands fail to deliver on new laws*. Available at: https://www.which.co.uk/news/article/how-long-will-your-smart-products-last-big-brands-fail-to-deliver-on-new-security-laws-atIYq4m4VP09

[13] Which? (2024), *Smart device brands must put privacy over profits.* Available at: https://www.which.co.uk/news/article/smart-device-brands-must-put-privacy-over-profits-at8Vq4t3VCn9

need to have a clear enforcement plan is vital to ensure that the market grows and develops in a way that protects privacy.

1) How the draft guidance must be clarified on the nature of harms

Definition of harms

Over the past two and a half years our Consumer Insight Tracker (a monthly poll weighted to be demographically representative of the national population[14]) has consistently shown that the majority of consumers (between 60-65%) are worried about how data about them is collected and used by businesses.[15]

Although flagged as 'not a comprehensive guide', the guidance lists the risks to people's rights and freedoms associated with the processing of personal information by IoT products and services. We also note the clarification that 'psychological harms' are included in potential detriment areas from Consumer IoT, alongside financial and physical threats.

The ICO says that: *'The harms can include people feeling they've lost control over their personal information. In some cases, this can lead to psychological distress (such as anxiety). Children may be especially susceptible to psychological harms from information revealing details about their preferences and personalities. People may lose trust in how their IoT products process personal information. This can lead to a chilling effect when people don't turn on the smart features."*[16]

We believe the definition and understanding of harms provided by the ICO is not clear enough, which could make it difficult for manufacturers to place the mitigation of harm at the heart of their product development programme as the ICO is calling on them to do. Psychological harm may include anxiety, as the ICO notes, but also shame, fear, anger, and sadness. Psychological distress can also negatively impact physical health and relationships, and therefore overall life satisfaction. For example, our 2021 research on detriment from the psychological impact on victims of fraud used an approach in HM Treasury's guidance on wellbeing analysis to estimate the wellbeing impact of online fraud at an average of £3,684 per victim, far exceeding the average financial loss of £600 per victim.[17]

We are concerned that awareness and understanding of these potential harms, particular to vulnerable consumers, is not broadly understood, and that can lead to Consumer IoT

---

[14] Which? (2024). *About the Consumer Insight tracker.* Available at: https://www.which.co.uk/policy-and-insight/article/about-the-consumer-insight-tracker-asxTG8k9XrQW

[15] The survey question is: 'How worried are you, if at all, about how data about you is collected and used by businesses? Very worried, Fairly worried, Not very worried, Not at all worried, Not applicable, Don't know.' The proportion of consumers worried is calculated by adding the proportion of respondents that are Very worried or Fairly worried. Which? (2024), *Consumer worries dashboard.* Available at: https://www.which.co.uk/policy-and-insight/article/consumer-worries-dashboard-akJMn5c4FKMv

[16] ICO (2025), *Draft Guidance for consumer Internet of Things products and services.* Available at: https://ico.org.uk/media2/2ptpdy3u/guidance-for-consumer-internet-of-things-products-and-services-all-0-0-22.pdf [p23]

[17] Which? (2023), *Scams and subjective well-being*. Available at: https://www.which.co.uk/policy-and-insight/article/scams-and-subjective-wellbeing-akBui5d71Rbb

manufacturers failing to fully comprehend such risks when they are designing products. We note that children are widely covered in the guidance, but there isn't a single reference to other types of vulnerable consumers that we can find in the draft guidance other than the vulnerability disclosure policy (which is mentioned in the context of security of personal information)[18].

We would recommend a detriment mapping exercise of psychological harms from Consumer IoT, and that this includes cases of tech abuse (that is, the use of technology to perpetrate domestic abuse[19]). This can then be used to help firms run effective Data Protection Impact Assessment (DPIA) exercises to mitigate against these harms.

Finally, we are concerned that mapped relationships in the guidance section on accountability currently appear to be quite binary and straightforward[20]. In fact, the IoT ecosystem is much more diffuse, with multiple companies, vendors, and service providers often involved in just a single product. Such a diffuse ecosystem poses the danger that the focus on consumer harms is diluted substantially to the point where it no longer has any real traction. This is even more pressing when supply chains involve companies from other regions and locations, with different data protection regimes and different conceptions of detriment, harm and consumer vulnerability.

2) How the draft guidance must be strengthened to address specific inadequacies

Exemptions

We largely accept the list of included and also exempted products.[21] However, we do question the exemption of smartphones and tablets. The first two devices are included under PSTI (albeit with a connectivity exemption on tablets), but no reason is provided by the ICO for exempting them. Smartphones, in particular, are what we'd call 'hub' or 'master' devices in the Consumer IoT ecosystem - in that they are used to control other connected devices in the consumer's smart products system via apps and other functionality. So we are concerned that the ICO's draft guidance does not ensure core controls are coordinated around them.

We were also disappointed by the lack of provisions for improving data protection in the automotive sector. We have previously reported on issues with data protection in the connected vehicles.[22] Like smartphones, cars are 'hub' devices in Consumer IoT, and so it is important to understand how manufacturers are being directed to use the best possible data protection standards.

---

[18] Ibid [p63]
[19] POST (2020), *Technology and domestic abuse.* Available at: https://post.parliament.uk/technology-and-domestic-abuse/
[20] Ibid [p18-27]
[21] Ibid [p5]
[22] Which? (2020), *We hacked a Ford Focus and a Volkswagen Polo*. Available at: https://www.which.co.uk/news/article/we-hacked-a-ford-focus-and-a-volkswagen-polo-aQ3dE0O2FLgQ

Permissions

In the section '*How do we inform people*?'[23], we would urge the ICO to include a general point around app permissions and how Consumer IoT vendors and developers should get fully informed consent for these. Our research has repeatedly exposed how Consumer IoT vendors are requesting excessive permissions from their apps[24]. One app we assessed recently requested more than 90; a comparable app requested 22 - but even that is also higher than all the major social media apps. Fine location permission requests are very common, as are requests for access to microphone and stored files.

We've found that most permissions are requested before set-up. Some permission requests relate to the functioning of the product/app but some are unnecessary and/or extensive at the point of set-up and this calls into question whether consent has been obtained properly.

We feel that it should not be placed in the hands of commercial companies to define best practice. It should be defined by the regulator.

We would be supportive of clear rules or guidelines on what is reasonable and excessive when it comes to app permission requests. Consumers should have more granular consent over what they do and don't want to agree to when it comes to permissions, and this should extend to the download stage of the app install process, as well as when the app is already installed on the device. The examples on page 37 of the guidance present some interesting ways to present individualised privacy settings that could be used as a starting point[25].

Consent journeys

We note the frequent use of examples in the guidance of how consent journeys can be improved, and welcome this as an approach to help increase business compliance. In the absence of a market-defining standard, it is vital that best practice examples are used to encourage good approaches to consent.

We note the ICO identifies the following points in the user experience where organisations should consider asking for consent. These include: *'during product set-up; when the IoT product collects personal information about a new person or when a new account is added; when a user enables a new product feature after initial set-up, and the feature requires consent for additional types of information for a new purpose (eg location data, health information); if a product update changes how personal information is processed; and if a young person becomes old enough to give consent for themselves*'[26]

We believe that consent should be expanded to the app download stage for any requested permissions. This should give granular control over what consumers do and don't want to grant in terms of potential access. This should be used in addition to the runtime permission requests that modern OS's are frequently introducing.

---

[23] Ibid [pp29-42]
[24] Which? (2025), *How much do apps know about you?* Available at: https://www.which.co.uk/news/article/how-much-do-apps-know-about-you-5-ways-to-improve-app-privacy-aJ4p38G3oS1x
[25] Ibid [p37]
[26] Ibid [p39]

We would also advise consideration of consent journeys to take into account vulnerable consumers. For example, while we note that multi-user consent journeys are considered, more thought needs to be given to consent in cases of potential tech abuse.

Finally, we would urge deeper testing and analysis of market interpretations of consent to give a clearer picture of how Consumer IoT vendors are interpreting their responsibilities and requirements. We note that there is an upcoming ICO project to investigate the Connected TV market and are keen to assist with the initiative using our own extensive expertise on smart TVs and consent journeys.

Consumer agency and ICO enforcement

We understand the need to empower consumers with various ways to enforce their data protection rights and gain greater control with Consumer IoT. Our research has found that people want meaningful control over their data, but feel powerless to engage with organisations who collect and use their data because of the power imbalance between consumers and organisations.[27] However, we are concerned that in absence of anything on ICO related enforcement, the guidance shifts the burden of enforcement on to consumers via the exercise of their data privacy rights. But consumers may not always be well-equipped or resourced to follow through with such measures - and may not even be aware of their rights.

Whilst consumer empowerment is part of the answer, in our view this is not a holistic approach. This is compounded as the guidance does not say anything on how the rules would be enforced if organisations fail to comply, or what would happen in the case of an identified market failure (in circumstances where the ICO in its draft impact assessment states that it seeks to help mitigate potential market failures around data protection and non-compliant processing of personal information via consumer IoT products)[28].

Data portability

When it comes to data portability, the guidance notes that manufacturers '*must transmit the personal information if it is technically feasible*'.[29] Data portability helps people unlock benefits from stored device data when they transition from one device to another, or attempt to integrate new devices into an existing system. Data portability can also strengthen competition by limiting companies' ability to lock consumers into their own brand ecosystem by making it hard for consumers to integrate devices from other brands, or stopping consumers from taking their data to a new device.

However, our testing has shown that it is extremely rare to see any data portability options presented to consumers. Even if they do contact the company to exercise this right, it is likely that they will receive data in a format that is barely usable, if they get a response at all. So while this right exists in theory, in practice consumers aren't able to exercise this right -

[27] Which? (2018), *Control, Alt or Delete? Consumer research on attitudes to data collection and use*. Available at: https://www.which.co.uk/policy-and-insight/article/control-alt-or-delete-consumer-research-on-attitudes-to-data-collection-and-use-aTS7R0Z87AI2

[28] ICO (2025), *Consumer Internet of Things - draft impact assessment*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/impact-and-evaluation/impact-assessment/consumer-internet-of-things-draft-impact-assessment-june-2025/

[29] Ibid [p74]

and if the ICO considers this right is useful to consumers, it is vital that rules and requirements for fostering true data portability in Consumer IoT are put forward.

3) How the draft guidance must be joined-up across the legislative and regulatory landscape

Privacy and the Consumer Rights Act

Based on our research, a significant majority of Consumer IoT products require consent for data protection processing in order for the user to fully access the functionality of the product that they have paid for[30].

If there is no clear signposting of such a consent requirement at the point of sale for Consumer IoT products, then if a consumer decides to object to processing and so views their product as not being 'as described, fit for purpose or of satisfactory quality', could they use this as grounds to access remedies under the Consumer Rights Act 2015[31]? This point, in our view, needs clarifying because of the transparency principle under the GDPR and the interaction with certain rights under the Consumer Rights Act 2015 (i.e. goods to be of 'satisfactory quality', 'as described' and 'fit for particular purpose') in circumstances where the processing of a user's personal data might be a fundamental characteristic of the product.

As previously noted, the ICO acknowledges that: *'The harms can include people feeling they've lost control over their personal information. [...] People may lose trust in how their IoT products process personal information. This can lead to a chilling effect when people don't turn on the smart features.'*[32] The draft guidance does not acknowledge this loss of the smart features as an additional consumer detriment.

Online advertising and 'legitimate interests'

We are encouraged to see the clarifications around consent requirements for storage and access technologies for online advertising purposes in Consumer IoT products. In particular, we note the following statement from the ICO: *'You might consider generating income through advertising necessary for your business but on a technical level, you can provide the service without any advertising'*[33].

The ICO must clarify whether processing data for online advertising is ever justified solely based on 'legitimate interests' as a lawful basis. If online advertising is not necessary to provide the Consumer IoT service, we believe 'legitimate interests' cannot be the lawful basis for any subsequent processing of information that is personal information. We would welcome clarification.

---

[30] Which? (2024), *Why is my air fryer spying on me? Which? reveals the smart devices gathering your data - and where they send it.* 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

[31] Consumer Rights Act 2015. Available at: https://www.legislation.gov.uk/ukpga/2015/15/contents

[32] Ibid [p23]

[33] Ibid [p16]

Location data and UK GDPR

As the ICO notes, location sensitivity (that is, user sensitivity about a device tracking their location, potentially up to a GPS level), is high among consumers[34]. In our recent survey of a nationally representative sample of 2,132 people aged 18+ in the UK in May 2025, consumers pointed to background location (68%) and fine/precise location (66%) as the data types they were most concerned about sharing[35]. Some 54% said that they were concerned or very concerned about coarse location sharing.

We are therefore pleased to see that the guidance clarifies that any vendor processing location data 'must comply with UK GDPR' where it amounts to personal information. However we also note that the guidance explains how PECR interacts with location data on terminal equipment: '*For example, the [PECR] rules on location data don't apply to GPS-based location information or data about connections with local Wi-Fi equipment*'[36]. We are concerned about the lack of clarity for the market. First, the draft guidance stops at saying that location data can be personal information but does not provide examples of what type of location data could amount to personal information[37].

Second, our research has shown widespread use of fine/precise location data by Consumer IoT devices, generally using GPS[38]. There must be absolute clarity on what must happen when processing location data (whether this is under the UK GDPR and/or PECR). As there is such a high level of public concern over location tracking by smart devices, the guidance should state clearly that fine and background location permission requests should only be issued if there is a specific and fully justified purpose. Too often a fine location permission is just requested by default, and this should not happen. The market must get to a position where fine location is not requested or used unless the consumer has explicitly consented to this.

PSTI and PECR

We note that the PSTI regulations are referenced in a number of places in the guidance; however, the guidance would benefit from clarification about whether failure to meet the PSTI regulations also denotes a breach of UK GDPR or PECR regulations. We recently tested a dashcam that had a default password and did not state a defined security update policy as required under PSTI. At present it is not clear whether the manufacturer of this product also fails to comply with its data protection obligations.

4) How the draft guidance must be expanded to address Implementation and enforcement

[34] Ibid [p11]
[35] Which? (2025), *How much do apps know about you?* Available at: https://www.which.co.uk/news/article/how-much-do-apps-know-about-you-5-ways-to-improve-app-privacy-aJ4p38G3oS1x
[36] Ibid [p17]
[37] Ibid [p11]
[38] Which? (2025), *How much do apps know about you?* Available at: https://www.which.co.uk/news/article/how-much-do-apps-know-about-you-5-ways-to-improve-app-privacy-aJ4p38G3oS1x

Standards development

One success of the introduction of PSTI regulations has been the positioning of the European Telecommunications Standards Institute (ETSI) 303 645 standard as a 'market defining' point in cyber security of Consumer IoT[39].

We encourage the ICO to create closer ties with the standards community and explore initiatives to use standards to create greater market consensus on technical measures for compliance. We would be open to being involved in such an initiative if it was to move forward.

Enforcement

We would like to see a clear plan for how this guidance will be monitored and enforced in the market. This is only very briefly covered in Section 7 'monitoring and evaluation' in the draft impact assessment[40]. The draft impact assessment states that this could potentially include establishing a central monitoring system, conducting post-engagement surveys with organisations, and exploring opportunities to monitor public understanding and comfort around use of their personal data by IoT products and services. However, there is nothing specific on the potential approach to enforcement.

We would like the ICO to commit to a review of the impact of the guidance to check how manufacturers are adhering to their responsibilities under data protection legislation. This could involve setting a strong threshold for harm reduction within a 1-year timeframe, otherwise the regulator would consider deeper market intervention measures.

If the ICO expects that the consumer IoT industry will raise its level to the guidance requirements, then there must be a clear statement of what will happen if this expectation is not met. The ICO's draft impact assessment notes a focus on growth in digital industries: we argue that consumer protection is to vital for economic growth[41] and supports innovation and investment[42]. If trust and consumer confidence increase as a result of data privacy compliance, so does the use of IoT Consumer products. Without this, companies may continue to underinvest in data protection and privacy measures, and so consumers will also continue to be exposed to harms.

About Which?

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

[39] DSIT (2019), *ETSI industry standard based on the Code of Practice*. Available at: https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-guidance-of-practice
[40] ICO (2025), *Consumer Internet of Things - draft impact assessment*. Available at: https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/impact-and-evaluation/impact-assessment/consumer-internet-of-things-draft-impact-assessment-june-2025/
[41] Which? (2024), *Consumer Policy for Economic Growth*. Available at:https://www.which.co.uk/policy-and-insight/article/consumer-policy-for-economic-growth-atjpZ9s9kQb6
[42] Which? (2022), *Consumer Protections and Economic Growth*. Available at: https://www.which.co.uk/policy-and-insight/article/consumer-protections-and-economic-growth-adyma5R8MF2I

our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with 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.

For more information contact:

Andy Laughlin
Principal Researcher/Writer
andrew.laughlin@which.co.uk

September 2025