



THE TRUST OPPORTUNITY:

EXPLORING CONSUMERS'
ATTITUDES TO THE
INTERNET OF THINGS



This new research from Consumers International and the Internet Society explored consumer perceptions and attitudes towards trust, security and the privacy of consumer Internet of Things (IoT) devices.

The survey of consumers in Australia, Canada, France, Japan, UK and the US aimed to find out what matters most to consumers when buying connected devices, and who is responsible for better privacy and security.

Contents

- 2 Executive Summary
- 4 About the partnership and project
 - Security and privacy opportunities in the consumer IoT market
 - Understanding attitudes and gathering opinions
 - Methodology
 - Defining connected devices
- 7 Research findings
 - 1. Immersed in privacy and security concerns
 - 2. Creepiness and distrust
 - 3. Low know-how
 - 4. Where does responsibility lie?
- 13 Building a trusted and safe consumer Internet of Things
- 14 Next steps
- 16 Annex – Full survey by IPSOS Mori

What we found:

- Connected devices are everywhere - but concerns about privacy and security remain.
- 63% of people surveyed find connected devices 'creepy' in the way they collect data about people and their behaviours
- This sentiment is echoed throughout the survey, with half of people across markets distrusting their connected devices to protect their privacy and handle their information in a respectful manner (53%).
- On top of not trusting the device itself to keep data secure, 75% of people agree there is reason for concern about their data being used by other organisations without their permission.
- The security concerns are serious enough to deter almost a third (28%) of people who do not own smart devices from buying one; security concerns are as strong a deterrent as the price of a device.¹
- People have concerns about security and privacy but do not know how to adapt and adjust device settings in a way that might allay these fears. 80% of people surveyed are aware of how to set and reset passwords, but only 50% are aware of how to disable the collection of data about users and their behaviours.

We see from the survey that a high number think that privacy and security standards should be assured by regulators (88%), followed by manufacturers (81%) and championed by retailers (80%).

¹ Please note, security concerns were as strong a deterrent as the price of a device in all markets except Japan.

28%

OF PEOPLE WHO DO NOT OWN A
SMART DEVICE, WILL NOT BUY ONE
DUE TO SECURITY CONCERNS

63%

OF PEOPLE FIND CONNECTED
DEVICES 'CREEPY'



75%

OF PEOPLE DISTRUST
THE WAY DATA IS SHARED

50%

OF PEOPLE KNOW HOW
TO DISABLE DATA COLLECTION

Given the level of concern amongst owners and non-owners, there is potential for companies to use high levels of privacy and security as a way to stand out from the crowd and build trust with current and future customers, while at the same time creating a more secure consumer IoT environment.

The results² also suggest consumers are thinking about the need for more formal regulation in the market. It is likely that this demand will grow as information about the risks associated with connected products becomes more widespread.

In response to this demand, companies should explore how to deliver assurances to consumers that their devices and services are helpful and useful without crossing the line into creepiness.

This could help them build trust in connected devices among consumers and potentially generate a competitive advantage.

ABOUT THE PARTNERSHIP AND PROJECT



Consumers International is the global membership organisation for consumer groups across the world. We bring together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We want consumers to get the best out of the digital economy and society without having to compromise on quality, care and fair treatment.



The Internet Society, founded by Internet pioneers, is a non-profit organization dedicated to ensuring the open development, evolution and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure and advocates for policies that enable universal access.

Consumers International and the Internet Society are working in partnership to deliver a better digital world, where everyone can benefit from digital innovation without compromising on their rights. We both believe that online security and privacy are key to online trust, which underpins all economic and social exchanges online.

The partnership brings together the best technical and policy knowledge related to IoT from the Internet Society and long-standing knowledge of consumer experiences and attitudes towards the digital economy and society from Consumers International.

The focus for our partnership has been on the growing market for consumer IoT as an important part of people's digital environment. We have been working towards effectively engaging consumers, governments and regulators, and businesses in the creation of a secure and trusted consumer IoT market. We want to enable consumer groups across the world to help drive demand for better security and privacy in consumer IoT products.

This research is a key part of this activity, exploring what consumers currently understand and feel about trust, security and privacy in the consumer IoT and how policy change, new business practice, standards development and enforcement, alongside awareness-raising among consumers, can bring positive change.

Security and privacy opportunities in the consumer IoT market

The rapid increase in products and services that are connected to the Internet are already transforming consumers' lives through connected energy grids, transport, home security and lifestyle appliances. Forecasts predict this technology is set to become part of everyday life with many products connected to the Internet by default.

Testing by consumer organisations³ has revealed dangerous weaknesses in a range of connected products, from children's toys and connected watches to connected TVs and fitness trackers. Such vulnerabilities create a risk of exposing the device itself (e.g. a connected home lock being disabled) and to personal data (e.g. information being shared with unauthorised third parties). Thinking beyond the harm to consumers, IoT vulnerabilities also create a risk of exposing networks (e.g. attacking the power grid of an entire country via connected webcams).

“ TESTING BY CONSUMER ORGANISATIONS
HAS REVEALED DANGEROUS WEAKNESSES
IN A RANGE OF CONNECTED PRODUCTS. ”

“ THE LACK OF CONSUMER TRUST IN
THE IOT MARKET COULD BE DETRIMENTAL
TO MANUFACTURERS AND RETAILERS. ”

As more types of connected-by-default devices and services become mainstream for consumers, these security and privacy issues are multiplied. These issues pose a threat not just to consumers' control over what happens to data about them, but also to consumer trust in IoT devices. The lack of consumer trust in the IoT market could be detrimental to manufacturers and retailers and as a result, it could stifle innovation within the industry. We believe there are opportunities for different stakeholders to address security and privacy issues in the IoT market and increase consumer trust.

Understanding attitudes and gathering opinions

Complementing our other activities with manufacturers, retailers and regulators within this partnership, this survey brings a valuable consumer perspective that allowed us to gather insights not only into how consumers perceive IoT devices, but also their levels of awareness and ideas around responsibility.

This study aimed to get a sense of consumers' attitudes to privacy and security when it comes to connected devices and explore to what extent consumers trust connected devices. Our other objectives were to understand what matters to consumers when buying connected devices and where they feel that the responsibility for better security and privacy lies.

³ See for example our Norwegian and Belgian members' activity:
<https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/>
<https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/>
<https://www.test-aankoop.be/action/pers%20informatie/persberichten/2018/hackable-home>
<https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/>

Methodology

The research was carried out by Ipsos MORI via their online panel survey which regularly surveys the general online population across the world.

We surveyed a sample of a minimum of 1,000 consumers in each of these countries: United States, France, Canada, Australia, United Kingdom and Japan between 1 March and 6 March 2019. We chose to conduct the survey online to ensure that the samples from each country were reflective of the general online population. People who are online are more likely to understand how such devices work. The study did not require people to own a connected device so that it also reflected the opinion of consumers who are considering or haven't bought a device.

Unravelling intricacies of consumer trust in connected devices and what underpins it can be a difficult task, especially within the setting of a quantitative survey that can be restricting in terms of the depth of insights. Concepts of both trust and connected devices can be abstract and vary in people's interpretation of each. The study tried to mitigate this difficult position by capturing consumers' attitudes towards trust in connected devices by prompting them with attitudinal statements about such devices. The statements were preceded by a definition and examples of connected devices.

Defining smart devices

For this research, we defined connected devices as everyday products and devices that can connect to the Internet using Wi-Fi or Bluetooth, such as connected meters, fitness monitors, connected toys, home assistants or gaming consoles.⁴

The definition excluded tablets, mobile phones and laptops; although they can be considered in technology terms 'connected devices', they are a lot more complex and apps allow them to perform many functions which in return generate more complex privacy and security issues than other connected devices. To avoid conflating the issues, the research focused on devices that do not have this added layer of complexity.



⁴ By prompting the respondents on what we mean by connected devices, we assure consistency and alignment on understanding, and thus ability to infer and generalize across markets. Translations of the original questionnaire was made to French (both Canadian and French version) and Japanese. Local proofing has been employed to ensure consistency in local differences, such as 'creepy', "concern", "risk" and examples of connected devices.



RESEARCH FINDINGS

1 IMMERSED IN PRIVACY AND SECURITY CONCERNS

Consumer IoT devices are widely used - the survey showed that 69% of participants across all markets own one or more devices such as connected meters, fitness monitors, connected toys, home assistants or gaming consoles.

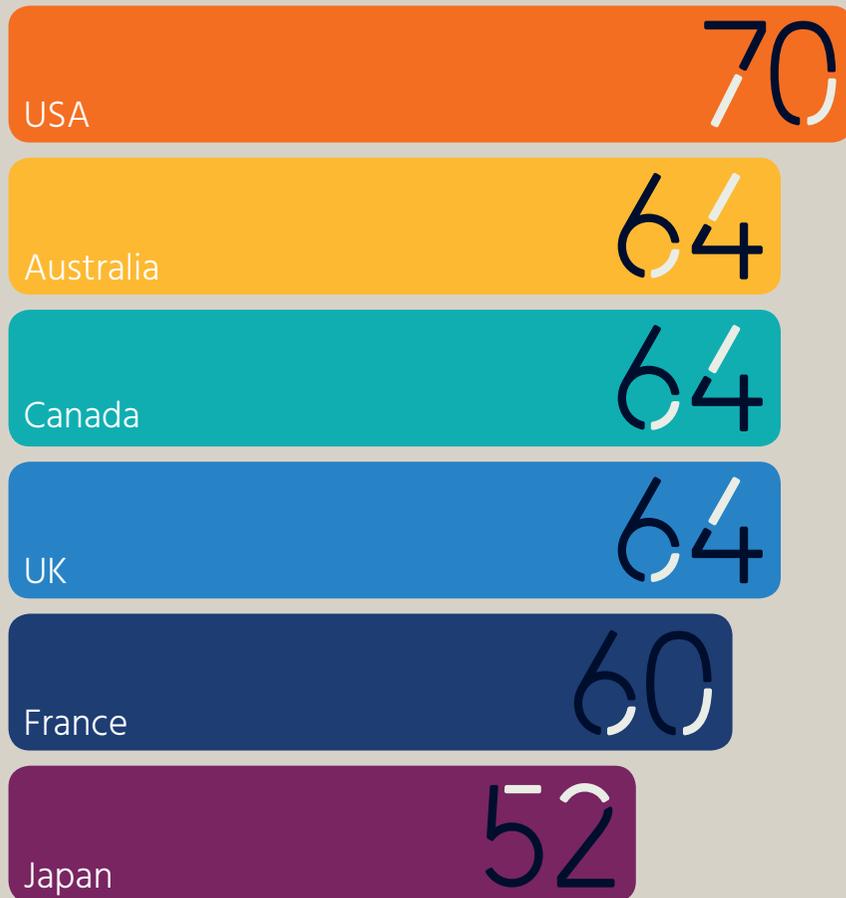
Our participants across all markets most commonly own gaming consoles, followed by home appliances and fitness monitors. On average, they own connected devices from at least two different categories (e.g. home appliances and connected wearables); however, this number is lower in Japan - where 46% do not own any Internet-connected devices.

We have also learned that high levels of connected device ownership does not indicate that people are satisfied with the privacy and security of these devices. On average, 65% of consumers across all markets report being concerned with the way connected devices collect and use personal data, with the US showing the highest concern levels at 70%.

On the other hand, consumers in France (60%) and Japan (52%) show less concern about the way these devices collect and use data, than the rest of the surveyed countries. For point of comparison we asked about other forms of technology, we found mobile apps (such as banking or health apps) had the highest levels of concern about the way personal data is collected (69%). The lowest level of concern found, was for tablets or laptops - which 62% of people are concerned about.

65% ACROSS ALL MARKETS ARE CONCERNED WITH THE WAY CONNECTED DEVICES COLLECT AND USE PERSONAL DATA.

CONCERN ABOUT THE WAY CONNECTED DEVICES COLLECT AND USE PERSONAL DATA:



In all countries, these concerns are shared by those who haven't purchased a device. We wanted to uncover whether consumer intentions to buy or not buy a connected device are related to their concerns about privacy and security. Although the most frequently mentioned barriers to purchasing a connected device across all countries are lack of need/use for them (63%) and cost (28%), the research also found that 28% of people who do not own and do not intend to purchase a connected device make this decision because of lack of trust in security and privacy.

The opportunity for trust?

It should come as no surprise that making useful, affordable, privacy and security-respecting devices will be popular with consumers, but we have not yet seen many companies voluntarily embrace strong privacy and security features in their products.

Given the level of concern amongst owners and non-owners, companies could use this as a way to stand out from the crowd and build trust with current and future customers and create a more secure consumer IoT environment. If we take into account how much focus manufacturers and retailers place on the price of a connected product as a way to influence consumers' purchasing behaviour, it is clear from our research that good privacy and security standards in an IoT device could be an equally important selling point and competitive differentiator.

2 CREEPINESS AND DISTRUST

Concepts and definitions such as trust, Internet of Things or even privacy and security can be difficult to explore among consumers because of their abstract nature. In particular, when trying to find out more about consumer trust in security and privacy of IoT devices we had to overcome the hurdle of trying to explain what we mean by ‘trust’.

People from different backgrounds and cultures can interpret a concept like trust in many ways. To mitigate the differences, we asked participants to express their opinion about a number of statements that could relate to their feelings of trust.

Our results showed that 63% of people agree that connected devices are creepy⁵ in the way they collect data about people and their behaviours, with French consumers being the most ‘creeped out’ (71%) and Japanese being the least (46%). This emotion was mirrored again when we asked about the possibility of other organisations accessing data from IoT devices about users without permission, for example advertisers misusing data consumers thought was being collected for a different purpose. In fact, three quarters of consumers across all surveyed countries were concerned about this practice when it comes to connected devices.

63% OF PEOPLE AGREE THAT CONNECTED DEVICES ARE CREEPY IN THE WAY THEY COLLECT DATA

“ BUILDING TRUST WITH CURRENT AND FUTURE CUSTOMERS IS ONE WAY COMPANIES COULD STAND OUT FROM THE CROWD. ”

Not only do consumers not trust the security of IoT devices to protect them from other parties accessing data about them, they even distrust the device itself. Across markets, over half of people tend to distrust their connected devices to protect their privacy and handle their information in a respectful manner (53%). In France, the number of people who distrust their devices to protect them is 63%.

Even though consumers own and engage with IoT devices, they do so with a cloud of suspicion around them and experience distrust towards the device on several levels.

The opportunity for trust?

There is a real opportunity for companies to rethink how they can nurture consumer trust in the IoT market. Companies, whether it is manufacturers or retailers, should explore how to deliver assurances to consumers that their devices and services are helpful and useful without crossing the line into creepiness which might contribute towards feelings of mistrust.

In practical terms, they can set proper expectations regarding what data is collected, how it is used and how it is secured. Companies can highlight features that can be controlled by the consumer, such as enabling or disabling data collection.

3 LOW KNOW-HOW

Exploring the concepts of privacy and security in connected devices among consumers has not been straightforward. It is difficult to separate the two and pinpoint where privacy ends and security starts. The two tend to work together on a higher conceptual level that most consumers do not engage with on a daily basis. For this reason, the research explored consumer awareness of the two concepts through privacy and security features of IoT devices.

We found that people have concerns about security and privacy but do not know how to adapt and adjust device settings in a way that might allay these fears. There is good knowledge of basic security best practices, such as setting and resetting passwords. 80% of people surveyed are aware of how to set and reset passwords and 68% of people are aware of automatic security updates from manufacturers. Knowledge of these features is essential for mitigating against hacks and lessening the impact of cyberattacks. However, a lot less is known about other settings in devices. Only 50% of consumers are aware of settings that control what data is collected and who it is shared with.

The research showed that in general consumers in Australia, UK, US and Canada are much more aware of security features in connected devices than consumers in Japan and France. However, the only security feature the four countries are as unsure about as France and Japan is disabling data collection on their connected device(s).

“ ONLY 50% OF CONSUMERS ARE AWARE OF SETTINGS THAT CONTROL DATA COLLECTION. ”

Even though consumers have low know-how of certain security features in connected devices, they have an appetite for security and privacy as wider concepts. They might not be so aware of some features but they have assessed that privacy and security are an important component of IoT devices and they, as consumers, should be aware of them. Our research showed that availability of information about the connected device's privacy and security is part of the purchase equation, with 77% of people across markets considering the availability of information about a connected device's privacy and security important for their decision to buy.

Among the surveyed countries, the numbers of US consumers taking privacy and security information about a connected device into account when making a purchase, was the highest (82%). By comparison, only 61% of French consumers look for this information when buying an IoT device, followed by Japanese consumers with 70%.



PERCENTAGE OF CONSUMERS WHO AGREED WITH EACH STATEMENT IN RELATION TO BUYING A CONNECTED DEVICE

HOW IMPORTANT ARE THESE FACTORS WHEN MAKING A
PURCHASE DECISION

THE CONNECTED DEVICE HAS
FEATURES THAT BEST SUIT MY NEEDS

86

THE CONNECTED DEVICE IS
AT AN AFFORDABLE PRICE

84

THE CONNECTED DEVICE IS
MADE BY A BRAND THAT I TRUST

80

THE CONNECTED DEVICE HAS POSITIVE
PRODUCT TEST RESULTS OR ONLINE REVIEWS

78

THERE IS INFORMATION AVAILABLE ABOUT THE
CONNECTED DEVICE'S PRIVACY AND SECURITY EITHER ON A
WEBSITE OR IN LITERATURE INCLUDED WITH THE PRODUCT

77

THE CONNECTED DEVICE IS SOLD
BY A RETAILER THAT I TRUST

72

THE CONNECTED DEVICE HAS A LABEL,
STICKER OR MARK THAT CERTIFIES IT IS
PRIVACY-PROTECTING AND SECURE

67

THE CONNECTED DEVICE IS
RECOMMENDED BY FRIENDS,
FAMILY OR COLLEAGUES

56

What influences consumers to buy or not buy IoT?

We investigated which factors were influential for consumers when they were deciding whether or not to buy a connected device. A list of eight potential factors were shown to respondents, and they were asked which they agreed with. The graphic opposite shows the percentage of consumers who agreed with each statement. These results show a blend of all of the eight factors were deemed important, indicating a complex decision-making process.

The opportunity for trust?

Improving knowledge of privacy and security features amongst consumers could go some way to helping consumers feel less concerned about how their personal information is used for things like marketing or service improvements.

4 WHERE DOES RESPONSIBILITY LIE?

Asking consumers to assign responsibility for security and privacy can be problematic. They often have only basic knowledge about issues around IoT and a lack of a wider picture of the IoT market. However, what people can do is to indicate whether they think they should have the responsibility as consumers.

Our survey showed that about 60% of people across markets think consumers should be responsible for safety and privacy on their connected devices. France had the lowest number of people wanting to take responsibility for security and privacy in IoT devices (48%). However, this number still shows that consumers as primary users of IoT devices share responsibility for security and privacy.

However, the majority of people agree that appropriate levels of privacy and security should be assured by regulators (88%), followed by manufacturers (81%) and favoured by retailers (80%). This trend differed slightly only in Japan where consumers had a stronger preference for setting legal obligations, such as regulation to secure standards for security and privacy in IoT devices.

These results do not come as a surprise following the previous findings showing that consumers do not have very sophisticated knowledge of security and privacy in IoT devices. The level of risk from devices and the complexity of securing devices contributes to consumers wanting regulators, manufacturers and retailers to uphold standards of privacy and security and to take more responsibility, as is the case with other mainstream activities that pose potentially high risks to individuals - such as the safety of air travel.

PERCENTAGE OF CONSUMERS WHO AGREED WITH EACH STATEMENT:

THERE SHOULD BE LEGAL PRIVACY AND SECURITY STANDARDS THAT MANUFACTURERS NEED TO COMPLY WITH

88

MANUFACTURERS SHOULD ONLY MAKE CONNECTED DEVICES THAT PROTECT PRIVACY AND SECURITY

81

RETAILERS SHOULD ENSURE THAT THE CONNECTED DEVICES THEY SELL HAVE GOOD PRIVACY AND SECURITY STANDARDS

80

CONSUMERS ARE MAINLY RESPONSIBLE FOR THEIR OWN PRIVACY AND SECURITY WHEN USING CONNECTED DEVICES

60

The opportunity for trust?

We predict that the demand for more formal regulation from consumers will grow as information about connected devices becomes more widespread and the media picks up on high profile hacks and security failings. Until this happens, retailers and manufacturers that demonstrate they have built-in security, privacy and trust by design have a great opportunity to stand out from the crowd and appeal to consumers.

BUILDING A TRUSTED AND SAFE CONSUMER INTERNET OF THINGS

This research gives us insight into what consumers know and feel about the privacy and security aspects of connected devices, and what more they would like to see to help build their trust and allay concerns. Understanding the consumer perspective and their experience of new products and services is crucial for developing effective policy, business and advocacy interventions.

These insights will also contribute to Consumers International and the Internet Society's ongoing work to build a trusted IoT environment that ensures security and respects privacy which includes work across the following areas:

Manufacturers and retailers:

- An Internet Society initiative, the **Online Trust Alliance (OTA)** addresses challenges in IoT to create a safer and more trustworthy connected world.
- Consumers International's **Trust by Design principles and accompanying guidelines** helping manufacturers create safe and trusted smart devices for consumers.
- **Minimum standards for tackling IoT security**, by Consumers International, the Internet Society and the Mozilla Foundation, launched a minimum set of requirements to keep connected consumer devices in the Internet of Things secure.

- **A joint call to retailers to adopt the Minimum Security Guidelines** and to commit to vetting all connected products they sell against these guidelines by the Internet Society, Consumers International, Mozilla and other partners.

Standards:

- Consumers International is an International Organisation for Standardisation Liaison member helping to develop a new standard Consumer protection: privacy by design for consumer goods and services standard (ISO/PC 317)⁶ which focuses on connected products.

International policy making fora:

- In May 2018, Consumers International co-hosted the second G20 Consumer Summit in Buenos Aires with a focus on the security of online. Following the event, the final leaders' declaration⁷ at the G20 called for improvements to security and privacy in consumer IoT, in particular for products marketed at or for children.

Consumer awareness:

- The Internet Society and Consumers International's **Connect-Smart campaign** raised awareness of the risks associated with connected products that fail to build in basic privacy and security features during the design stage.



““ ALTHOUGH LARGE NUMBERS OF CONNECTED DEVICES ARE NOW IN PEOPLE’S HOMES, CONSUMER DISTRUST IN IOT PERSISTS.””

Internet of Things devices enhance the day-to-day activities of users around the world by providing benefits such as greater convenience, more streamlined services and better information.

However, the results of this survey demonstrate that consumer distrust in IoT persists. In fact, survey findings show in some cases this distrust has discouraged consumers from purchasing connected devices.

While there are many factors at play when it comes to consumer trust in connected devices, manufacturers and retailers can achieve significant impact by adopting IoT privacy and security standards. In doing so, trust becomes embedded in the design and sale of IoT devices; consumers can more confidently buy and enjoy safer IoT devices; and manufacturers and retailers can further differentiate as leading brands that proactively protect consumers’ best interests.

““ CONSUMERS BENEFIT WHEN TRUST BECOMES EMBEDDED IN THE DESIGN AND SALE OF IOT DEVICES.””

The Internet Society and Consumers International have been working together, and with other partners, to provide resources to support manufacturers and retailers in the adoption of IoT privacy and security standards.

If you are a manufacturer or retailer interested in learning more, you can find more information from the Internet Society on their Trust by Design initiative, or from Consumers International for a number of IoT guidelines and checklists.



ANNEX SURVEY BY IPSOS MORI

(Ask all)

Q1. We are conducting research on ‘connected devices’ in the home. By this, we mean everyday products and devices that can connect to the Internet (not including tablets, mobile phones or laptops).

Which, if any, of the following types of Internet-connected device(s) do you have in your household:

Randomise codes 1-8, multicode 1-8.
Code 9, 10 are single code

1. Connected appliances (for example gas/electric meters, printers, speakers, TVs, refrigerators, thermostats or robotic floor cleaners)
2. Connected wearables (for example smart watches)
3. Fitness monitors (for example Fitbit)
4. Home assistants (for example Amazon Alexa or Google Assistant)
5. Gaming consoles connected to the Internet (for example Xbox, PlayStation 4 or Nintendo Wii U)
6. Connected home security systems (for example SimplySafe)
7. Connected toys, baby monitors or GPS child trackers (for example Hello Barbie, Furby Connect, Phillips Avent, Amber Alert)
8. Car with connected system (for example Audi Connect, Lexus Enform, Ford SYNC3)
9. None of these
10. Don't know

(Ask all)

Q2. How likely or unlikely are you PERSONALLY to buy a connected device in the next 12 months?

Connected devices are everyday products and devices that can connect to the Internet using wifi or bluetooth (not including tablets, mobile phones or laptops).

Forward and reverse scale 1-7, single code

1. Certain to
2. Very likely to
3. Fairly likely to
4. Neither likely nor unlikely
5. Fairly unlikely
6. Very unlikely
7. Certain NOT to
8. Don't know

(Ask if 5 to 7 at Q2)

Q3. Why is that?

Randomise codes 1-5, multicode 1-5.
Code 6 is single code

1. Do not trust the privacy or security of the device
2. Do not have any need/use for them
3. Too expensive
4. I have not really considered them
5. I don't have enough information about what to buy
6. No specific reason

(Ask all)

Q4. Here is a list of different products and devices. For each one, how concerned, if at all, are you about the way they collect and use personal data?

Even if you do not own the products or devices, we are still interested in your impressions.

Randomise statements (rows), forward/reverse scale 1-4 (columns), single code per row

Columns

1. Very concerned
2. Fairly concerned
3. Not very concerned
4. Not at all concerned
5. Don't know

Rows

1. Mobile phones
2. Tablets or laptops
3. Internet-connected devices (such as appliances, home assistants like Amazon Alexa or Google Assistant, toys, baby monitors, etc.)
4. Apps such as those found on Smart phones or tablets (such as banking, health, etc.)

(Ask all)

Q5. Connected devices are everyday products and devices that connect to the Internet using wifi or bluetooth (not including tablets, mobile phones or laptops).

To what extent do you agree or disagree with the following statements about connected devices...

Randomise statements (rows), forward/reverse scale 1-5 (columns), single code per row

Columns

1. Strongly agree
2. Somewhat agree
3. Neither agree nor disagree
4. Somewhat disagree
5. Strongly disagree
6. Don't know

Rows

1. Connected devices make people's lives easier
2. Connected devices are creepy in the way they collect data about people and their behaviours
3. People who are not using connected devices should give them a try
4. People using connected devices should be concerned about their data being used by other organisations without their permission
5. People using connected devices should worry about the risk of "eavesdropping" (devices are being accessed without their knowledge or permission)

(Ask all)

Q6. Connected devices are everyday products and devices that can connect to the Internet using wifi or bluetooth (not including tablets, mobile phones or laptops).

How much, if at all, do you trust connected devices to...

Randomise statements (rows), forward/reverse scale 1-4 (columns), single code per rows

Columns

1. A great deal
2. A fair amount
3. Not very much
4. Not at all
5. Don't know

Rows

1. ...protect users' data so no one else can access it
2. ...not to be a risk to users' personal privacy
3. ...ensure that data collected about users and their behaviours handled responsibly and transparently
4. ...ensure that sufficient security is in place to allow you to change the privacy and security settings without impacting the usage

(Ask all)

Q6. Connected devices are everyday products and devices that can connect to the Internet using wifi or bluetooth (not including tablets, mobile phones or laptops).

How would you describe your awareness of the following possible privacy and security features on connected devices?

Randomise statements (rows), forward/reverse scale 1-4 (columns), single code per row

Columns

1. Yes – fully aware of this/how to do this
2. Yes – aware of this/how to do this, but not in detail
3. No – not aware of this/how to do this
4. Never heard of this
5. Don't know

Rows

- a) Ability to disable the collection of data for users and their behaviours
- b) A User Agreement that explains if data is being collected and if it is being shared with a third party
- c) Encryption to protect against unauthorized access to data about the users and their behaviours
- d) Option to set and reset passwords
- e) Automatic security updates from the manufacturer

(Ask all)

Q7. Connected devices are everyday products and devices that can connect to the Internet using wifi or bluetooth (not including tablets, mobile phones or laptops).

How important, if at all, do you think each of the following factors would be to you personally when making a decision about whether or not to purchase a connected device?

Randomise statements (rows), forward/reverse scale 1-5 (columns), single code per row

Columns

1. Very important
2. Fairly important
3. Not very important
4. Not at all important
5. Don't know

Rows

1. The connected device is made by a brand that I trust
2. The connected device has positive product test results or online reviews
3. The connected device is recommended by friends, family or colleagues
4. The connected device is at an affordable price
5. The connected device is sold by a retailer that I trust
6. The connected device has a label, sticker or mark that certifies it is privacy-protecting and secure
7. The connected device has features that best suit my needs
8. There is information available about the connected device's privacy and security either on a website or in literature included with the product (This can be information from the retailer, manufacturer or a government consumer protection agency)

(Ask all)

Q8. Connected devices are everyday products and devices that can connect to the Internet using wifi or bluetooth (not including tablets, mobile phones or laptops).

To what extent do you agree or disagree with the following statements about connected devices?

Randomise statements (rows), forward/reverse scale 1-5 (columns), single code per row

Columns

1. Strongly agree
2. Somewhat agree
3. Neither agree nor disagree
4. Somewhat disagree
5. Strongly disagree
6. Don't know

Rows

1. There should be legal privacy and security standards that manufacturers need to comply with
2. Manufacturers should only make connected devices that protect privacy and security
3. Retailers should ensure that connected devices they sell have good privacy and security standards
4. Consumers are mainly responsible for their own privacy and security when using connected devices