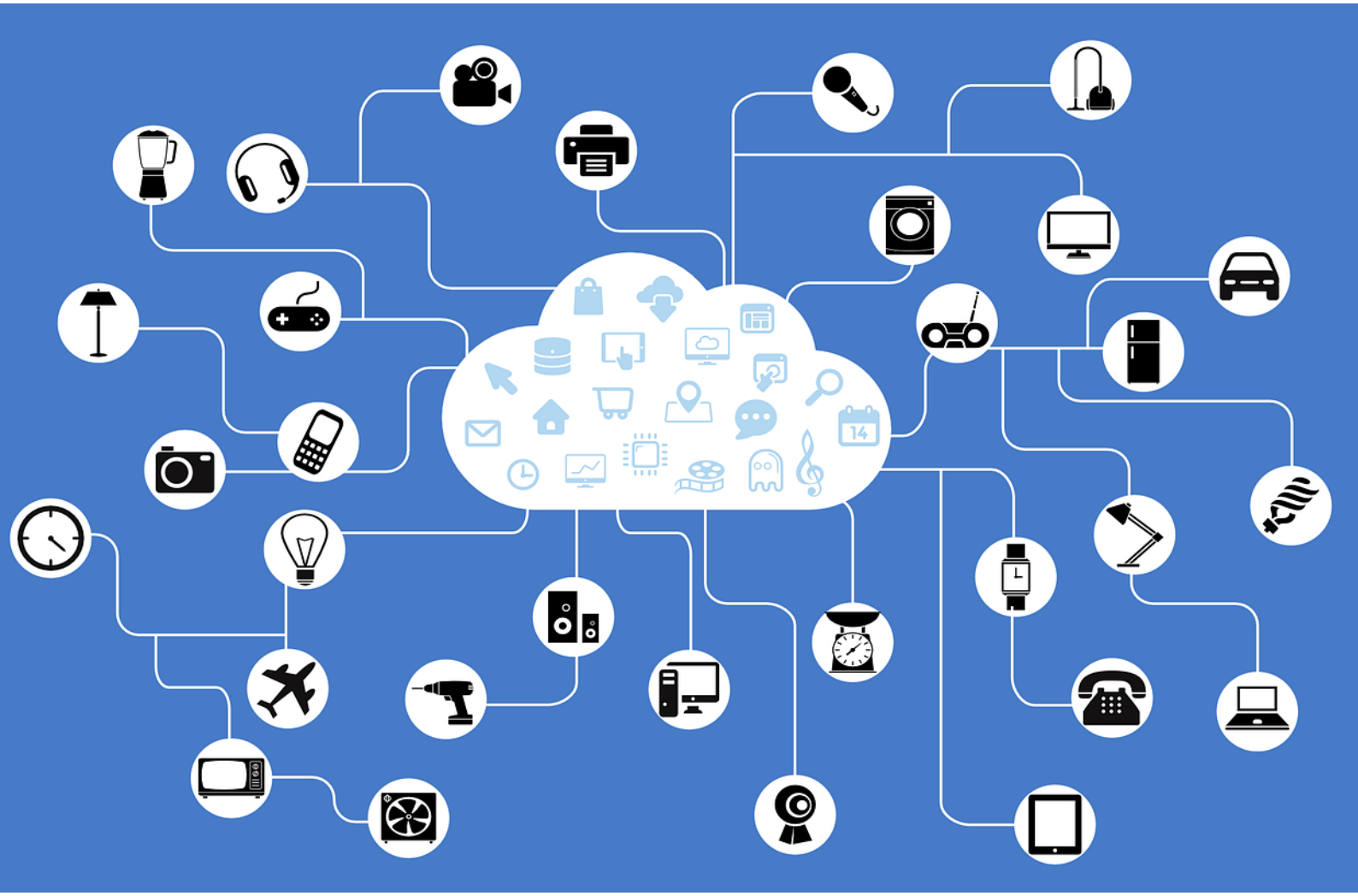
Consumer Survey on App Stores, Internet of Things (IoT), and Connected Places

A report for the Department for Science, Innovation, and Technology (DSIT)



LE London Economics

February 2024

About London Economics

London Economics is one of Europe's leading specialist economics and policy consultancies and has its head office in London.

We advise clients in both the public and private sectors on economic and financial analysis, policy development and evaluation, business strategy, and regulatory and competition policy. Our consultants are highly qualified economists with experience in applying a wide variety of analytical techniques to assist our work, including cost-benefit analysis, multi-criteria analysis, policy simulation, scenario building, statistical analysis, and mathematical modelling. We are also experienced in using a wide range of data collection techniques including literature reviews, survey questionnaires, interviews and focus groups.

Head Office: Somerset House, New Wing, Strand, London, WC2R 1LA, United Kingdom.

w: londoneconomics.co.uk e: info@londoneconomics.co.uk X: @LondonEconomics
t: +44 (0)20 3701 7700 f: +44 (0)20 3701 7701

Authors

Calum Kennedy Economic Analyst

Tiffany Head Senior Economic Consultant

Wouter Landzaat Senior Economic Consultant

Dr Charlotte Duke Partner

Table of Contents

Executive Summary

Background

The Department for Science, Innovation and Technology (DSIT) commissioned London Economics and YouGov to conduct two consumer surveys, one covering consumer Internet of Things (IoT) devices and connected places technology, and one covering apps and app stores. The overall purpose of this research is to gain deeper insights into consumer perceptions, attitudes and behaviours related to app stores, consumer IoT devices, and connected places technology.

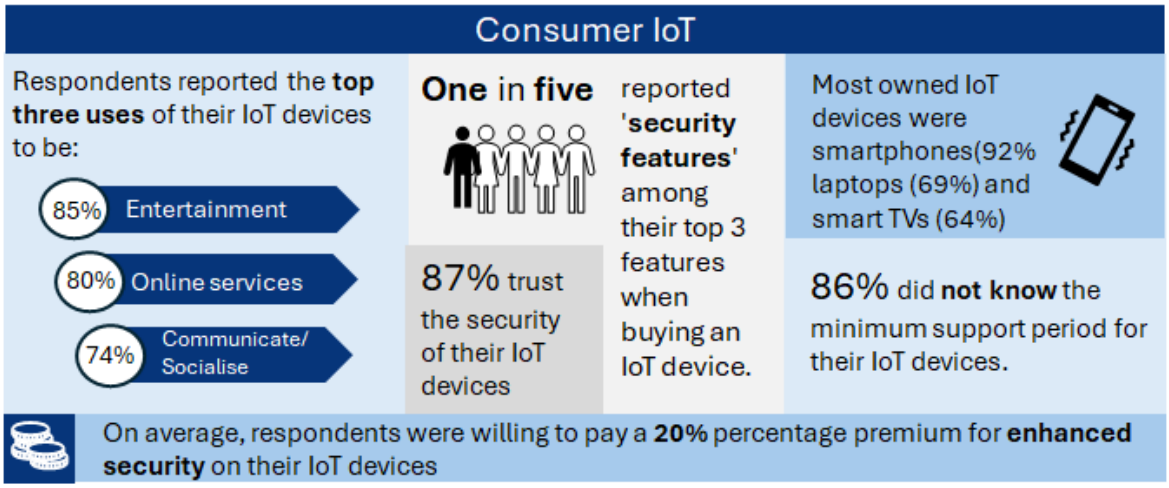
YouGov undertook two nationally representative online surveys from 25th August to 15th September 2023. The consumer IoT devices and connected places technology survey had a total sample size of 3,352 UK adults. The apps and app stores survey had a sample size of 3,796 UK adults.

The insights developed in this report will support the Department's work and inform the development of policy under the Government's National Cyber Strategy (published in 2022) which details plans to ensure the UK's confidence, capability, and resilience in the rapidly evolving digital landscape.

Main findings

The findings from the surveys were similar across all consumer groups. Where there are differences between groups (e.g. by age, income, education level etc.), these are highlighted in the report.

Consumer IoT



Consumer IoT device ownership and usage

The most commonly owned consumer IoT devices included smartphones (92%), laptops (69%), and smart TVs (64%). Respondents reported that they mostly used their IoT devices for entertainment (85%), accessing services online (80%), and helping to communicate or socialise (74%). Around 60% of respondents who had a disability which limited their day-to-day activities felt that consumer IoT devices had helped to manage their condition.

Purchasing behaviour

The most popular mode of purchasing devices was online via the website of a physical store (65%). Older respondents, particularly those over 65 years old, predominantly prefer purchasing directly from physical stores.

Respondents were also asked about their behaviours around upgrading, replacing or disposing of their IoT devices. For more expensive IoT devices (such as smart fridges and TVs), most respondents reported replacing these devices every 5-10 years. For connecting the home products (e.g. smart speakers and lightbulbs) and consumer lifestyle products (e.g. smartphones and watches), most reported replacing these items more regularly – every 2-5 years. Around one third of respondents reported that they actively consider environmental factors when disposing of their IoT devices. This proportion was higher amongst older people.

Consumer attitudes towards IoT security

Most respondents (87%) reported that they trust the security of their IoT devices at least to some extent. Respondents were also asked about the security information related to their IoT devices. Most respondents did not know the minimum support period for their IoT devices (86%). However, only 19% of respondents stated that they did not know where they would expect to find security information. This finding indicates that around four in five consumers have an idea of where they can find security information for their IoT devices.

Women and respondents with a lower level of education were more likely to report that they did not know where to find security information for their devices. When asked about their perceptions on where the responsibility for product safety and security lies, respondents generally felt that manufacturers had more responsibility than retailers. Specifically, 78% of respondents felt manufacturers had the same amount, or more, responsibility for product safety and security than retailers.

Consumer behaviours towards IoT security

Respondents were asked about the top three characteristics that were important to them when purchasing an IoT device. Price was reported as the most important characteristic by 35% of respondents, followed by ease of use (17%) and range of available functions (14%). Around one in five respondents put security features in their top three features. Consumers perceived the minimum device support period and customer support reviews to be the least important characteristics.

Respondents were asked to state the percentage premium they would be willing to pay for an IoT device in return for a given percentage reduction in the number of security incidents or breaches relating to that device each year. On average, respondents were willing to pay a 20% percentage premium for enhanced security, with a slightly higher premium for 'consumer lifestyle' devices.

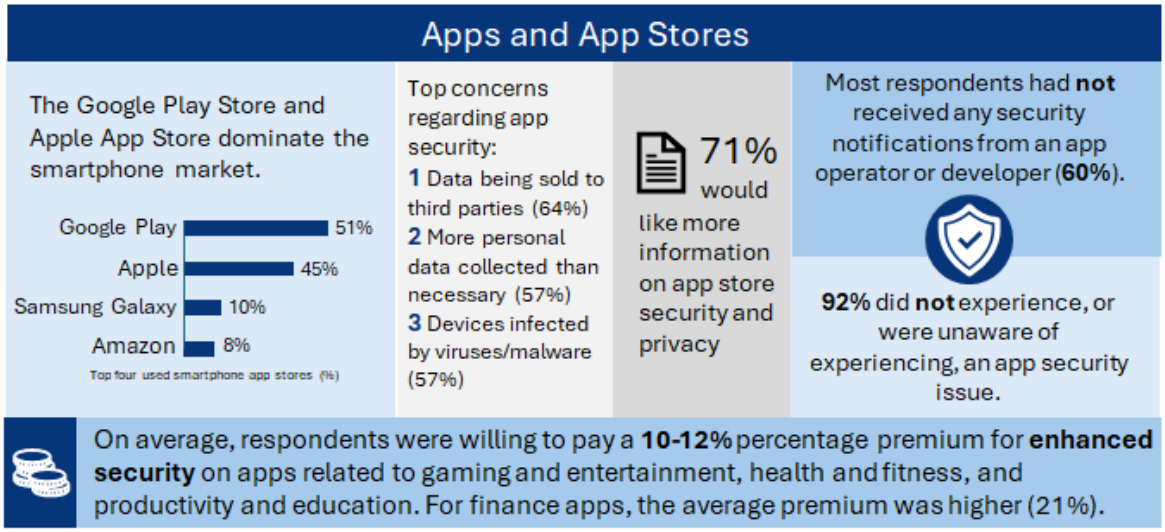
Consumer IoT security issues

The survey asked respondents about their experience with security issues relating to their consumer IoT devices. Most survey respondents (84%) reported that they were unaware of experiencing any security issues. Of those that did, laptops were the most common device for which respondents had experienced a security issue.

Among respondents who reported they had experienced a security issue, the most common type of issue was receiving a security notification from the IoT device (64%), with the most prevalent impacts being the time lost in resolving the issue (42%) and emotional distress (22%).

Evidence from the survey suggested that experiencing a security issue with an IoT device changed respondents' awareness and behaviours around IoT device security. Nearly three quarters (71%) reported a higher level of awareness of IoT device security. Behaviours included changing their device password (59%), installing device security updates (47%), and disconnecting the device from the internet (26%). In general, a majority (60%) of these respondents said that they now check security features before buying consumer IoT products.

Apps and app stores



Consumer device ownership and app store usage

Consumer device ownership was similar to that found in the consumer IoT survey, where ownership was highest for smartphones (95%), laptops/desktops (80%) and smart TVs (61%). Among smartphone users, the Google Play Store was the most used app store (52%). For laptop/desktop users the most used app store was the Microsoft Store (35%), while for smart TV users, around half of respondents reported only using the pre-installed apps on their TV.

Consumer attitudes towards app security

The survey explored consumers' knowledge of app security information, concerns regarding app security, and their perceptions and experiences with app store operators and app developers.

Respondents were divided on the ease of finding app security information, with around a third never having attempted to do so. Generally, consumers expressed a desire for more privacy and security information, especially amongst those that said they found it hard to locate information.

Top concerns regarding app security were consumers' data being sold to third parties (64%), apps collecting more personal information than they need (57%), and their devices being infected by viruses or malware (57%). A higher level of education was correlated with greater concern about app security issues.

Respondents were asked the extent to which they believed app store operators and app developers are doing enough to protect users. The majority reported not knowing what either operators or developers are doing to protect their users (58% and 61%, respectively). Respondents were also asked about their experiences with security notifications from operators or developers. Most respondents had not received any security notifications from either platform in the past year. Of those that did, the most common channel was through in-app alerts (49% for operators, 51% for developers) or emails. The notifications typically contained instructions on how to protect themselves.

Consumer behaviours towards app security

Respondents were asked to specify what actions they took before and after downloading apps on their device. Before downloading apps, 55% read reviews and 32% checked how the app uses data. After downloading apps, 40% install updates and 33% check for updates. Only 8% of respondents reported taking no action before or after downloading apps.

Respondents were asked to state the percentage premium they would be willing to pay for improvements in cyber security when purchasing apps. Respondents were asked to report their willingness to pay separately for four different categories of app – gaming or entertainment, finance, health and fitness, and productivity and education. On average, respondents reporting willingness to pay a 10-12% premium for gaming or entertainment, health and fitness and productivity and education related apps. For finance apps, the average premium was higher at 21%.

Consumer experiences and impacts of cyber security issues

Most respondents reported not experiencing, or being unaware of experiencing, an app security issue (92%). Younger respondents (18-25) were twice as likely to report experiencing issues than older respondents (over 65s).

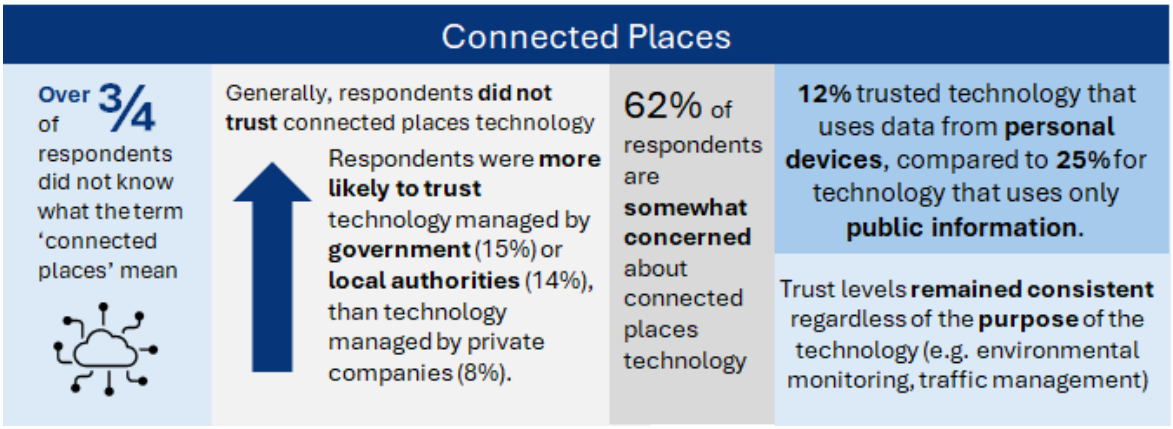
Of those that did report experiencing an issue, common impacts included loss of trust in the app (41%) and time lost resolving the issue (30%). In terms of how people responded to the issue, around half of consumers reported changing their approach to app security, with nearly a third taking additional actions when downloading an app. These actions include checking privacy and security features (59%) and reading customer reviews before downloading an app (66%). Around one in five people reported that they did not download apps anymore.

Consumer attitudes to the Code of Practice for app store operators and app developers

To test consumer understanding of the updated Code of Practice and its implications for security and transparency, respondents were presented with information about the Code, including some of its key requirements for app store operators and developers. Generally, respondents reported they understood the information (around 70%), with slightly higher reported comprehension amongst younger age groups.

Around 80% of respondents indicated that they would prioritise using an app store if it had publicly stated that it had implemented the security and privacy requirements set out in the updated Code of Practice.

Connected places



Awareness of connected places/smart cities

Most respondents reported being unfamiliar with the concept of connected places (77%), with higher awareness amongst higher income households. Similarly, most respondents (72%) reported not having seen examples of connected places technology (e.g. smart lamp posts which control light via sensors and data driven traffic management).

Trust in connected places technology

Generally, respondents did not trust connected places technology. Consumers were generally more trusting of technology managed by the government compared to technology managed by private companies, although only marginally. In terms of the function of connected places technology, consumers were most trusting of technology for the purpose of environmental monitoring. Consumers were less trusting of technology which gathers data from personal devices rather than solely public data.

Concerns around connected places technology

Most respondents (62%) reported being somewhat or a little concerned about connected places technology. Exploring the relationship between awareness and concern, the findings provided some evidence that the more examples people saw of connected places technology, the more concerned they were.

Cross-cutting themes across consumer IoT, apps and app stores, and connected places

Trust in the security of technology

Respondents generally exhibit a high-level trust in, and usage of, consumer IoT devices and app stores. However, respondents' level of knowledge regarding privacy and security aspects of these technologies was relatively low. For example, while 87% of respondents expressed some level of trust in the security of their IoT devices, and the majority of respondents reported using app stores (93% of smartphone owners), most were unaware where to find security information for their IoT devices or apps. These findings could indicate that consumer trust may not be grounded in a comprehensive understanding of the privacy and security measures related to their apps or devices.

The connected places component of the survey generated different findings with regards to consumer attitudes towards security. Consumers were generally concerned at least to some extent about the security of connected places and reported a high degree of mistrust in connected places technology.

Changes in behaviour following a security issue

The survey found that experiencing a security issue with an IoT device or app prompted people to change their behaviour towards device or app security to some extent. For example, 60% of respondents who experienced a security issue with an IoT device now consider the security features of a device before purchasing it. Similarly, among people who experienced an issue with an app, 65% reported that they now took additional security measures when downloading apps. These findings suggest that experiencing issues with consumer IoT devices or apps leads to tangible changes in purchasing and usage behaviours.

1 Background and methodology

1.1 Background and policy context

The Department for Science, Innovation and Technology (DSIT) commissioned London Economics and YouGov to conduct a consumer survey covering App Stores, consumer Internet of Things (IoT) devices, and connected places technology. The overall purpose of this research is to gain deeper insights into consumer perceptions, attitudes and behaviours related to app stores, consumer IoT devices and connected places technology.

The insights developed in this report will support the Department's work and inform the development of policy under the Government's National Cyber Strategy (published in 2022) which details plans to ensure the UK's confidence, capability, and resilience in the rapidly evolving digital landscape.

Consumer IoT Devices

The Internet of Things (IoT) refers to a network of connected devices that communicate with each other. This research focuses on consumer IoT, which refers to internet-connected devices available for purchase by consumers. Examples of consumer IoT devices include smartphones, laptops/desktops, smart watches, smart speakers, connected children's toys, and baby monitors.

Consumer IoT devices have brought a new era of connectivity and convenience. However, one of the main issues with these devices is a lack of adequate built-in security at the design stage, which can increase vulnerability to cyber-attacks. In response, guidance for manufacturers such as the UK's Code of Practice on Consumer IoT Security[1] and the ETSI EN 303 645 European Standard[2] has been developed to promote good practice in security for connected consumer devices. Additionally, the Product Security and Telecommunications Infrastructure (PTSI) Act 2022[3] was introduced in the UK to address cyber security issues with connected devices.

The survey on consumer IoT devices gathers evidence on consumer perceptions, attitudes, behaviour, and experiences with their IoT devices, informing future policy development in the connectable IoT landscape.

App Stores

The increasing reliance on apps for everyday life and work across various devices including smartphones, laptops, and wearable technology, has raised concerns about user safety, privacy and security. The UK Government conducted an investigation of the app ecosystem and found a range of threats relating to malicious and poorly developed apps.[4]

In response, the Government developed a Code of Practice, applicable to both app store operators and app developers, outlining a set of minimum requirements for security and privacy standards.[5] These minimum requirements include providing users with important security and privacy

[1] Department for Science, Innovation and Technology, Department for Digital, Culture, Media and Sport (2018) Code of Practice for Consumer IoT Security

[2] ETSI (2020) Final draft ETSI EN 303 645. CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

[3] Department for Science, Innovation and Technology, Department for Digital, Culture, Media and Sport (2021) The Product Security and Telecommunications Infrastructure (PSTI) Bill – product security factsheet

[4] National Cyber Security Centre (2022) Threat report on application stores

[5] Department for Science Innovation and Technology (2022) Code of Practice for App Store Operators and App Developers

information in an accessible way, taking appropriate steps when a security issue arises, keeping apps updated, and only allowing apps that meet baseline privacy and security requirements onto app stores.

Given that adherence to the Code is voluntary, it is necessary to monitor the uptake of these requirements. The app store survey conducted by London Economics and YouGov explores consumers' experiences relating to many of the Code's key principles. The research will contribute towards understanding progress towards these principles and inform next steps for the Code.

Connected Places

Connected places, often referred to as 'smart cities' in urban areas, involve the use of digital technology to build digital connections in physical spaces. This involves using a network of devices and sensors to improve the functionality of various aspects of the physical space, including transportation, public services, utilities, and the environment.

Examples of connected places technology include adaptive traffic lights based on traffic patterns observed through mobile phone data and smart lamp posts which control light via sensors. Connected places rely on a network of connected devices which collect, analyse, and share data, which means that connected places can be vulnerable to cyber security threats. The current market in the UK for connected places is relatively small but growing, which implies the existence of greater potential cyber security risks in the future.

The connected places survey gathers evidence on consumer awareness and perceptions of connected places or 'smart cities', including exploring concerns around the cyber security risks and the level of trust in connected places technology.

1.2 Survey methodology

London Economics commissioned YouGov to undertake two nationally representative online surveys. One survey covered apps and app stores and was based on a sample of 3,796 UK adults. The second survey covered consumer IoT devices and connected places and had a total sample size of 3,352 UK adults.[6]

Both questionnaires were designed by London Economics. Drafts were received by YouGov which were reviewed and updated to ensure the questions would translate successfully online. The surveys were hosted in the bespoke YouGov online survey platform.

The sample was drawn from the YouGov online panel which consists of over 2.5 million adults in the UK. The sample for the surveys was designed to be representative of adults aged 18+ within the UK. To obtain a representative sample, recruitment quotas were placed on age, gender, social grade, ethnic background, urban/town/rural status, and region. A summary of those targets and achieved sample used in both surveys are provided in the table below.

[6] It should be noted that there are individuals without an online presence who may still engage with connected places but were not captured in this survey as it was conducted exclusively online.

Table 1 Survey quota targets and achieved sample sizes

Demographic	Breakdown	Target	Achieved (App and app store survey)	Achieved (Consumer IoT and Connected Places survey)
Age	18-29	22.5%	17.9%	18.0%
	30-39	15.9%	20.1%	18.3%
	40-49	17.3%	16.1%	17.0%
	50-59	15.8%	16.2%	17.1%
	60-69	13.5%	14.9%	14.4%
	70-99	15.0%	14.6%	15.1%
Gender	Male	48.7%	44.4%	44.7%
	Female	51.3%	55.6%	55.3%
Social Grade	A, B	21.9%	27.1%	26.1%
	C1	29.7%	29.6%	31.6%
	C2	15.0%	14.1%	15.7%
	D, E	33.4%	29.3%	26.6%
Ethnic background	Any white background	82.0%	88.3%	84.2%
	Multiple ethnic background	3.0%	2.0%	2.9%
	Any Asian background	9.0%	5.5%	8.1%
	Any black background	3.0%	2.6%	2.8%
	Any other background	3.0%	1.5%	1.9%
Urban/town/rural status	Urban	82.0%	77.4%	80.9%
	Town and Fringe	9.0%	10.9%	9.5%
	Rural	9.0%	11.7%	9.6%
Region	North East	4.1%	4.3%	4.1%
	North West	11.0%	10.4%	11.1%
	Yorkshire and the Humber	8.3%	7.9%	8.6%
	East Midlands	7.2%	6.8%	7.5%
	West Midlands	8.8%	8.2%	9.3%
	East of England	9.3%	7.9%	8.9%
	London	13.0%	11.5%	12.6%
	South East	13.7%	13.7%	14.1%
	South West	8.5%	8.8%	8.8%
	Wales	4.8%	4.1%	4.8%
	Scotland	8.5%	9.1%	8.7%
	Northern Ireland	2.8%	7.2%	1.5%

Source: YouGov

Once the sample had been drawn, an invitation was sent by email with an embedded link to the survey. All respondents participated in the survey in the same way and the YouGov panel management team ensured the invitations to the survey were consistently and professionally managed. Only respondents who were invited to take part could do so. The surveys could not be undertaken in any other way.

Both surveys were piloted with 100 respondents. The pilot data was used to check the integrity of the surveys ensuring that length, routing, question performance and respondent comprehension were working as intended. Based on this, minor updates were made to the surveys.

Both surveys were conducted online using the YouGov bespoke online survey platform. The fieldwork was completed between 25th August and 15th September 2023.

Once the data had been processed, YouGov applied a weighting which adjusts the contribution of individual respondents to aggregated figures and is used to ensure surveyed populations are representative. For both the Apps and app stores and IoT surveys, findings were weighted to ensure the data represented the national profile of adults across the UK by age, gender, social grade, ethnic background, urban/town/rural status, and region. However, due to the large sample size of the surveys and the use of YouGov's representative online panel, this did not change the sample sizes very much.[7]

Analysis by socio-demographic groups

Throughout the report, where differences between socio-demographic groups are reported, the difference is statistically significant at the 5% level using a two-sided t-test. The two-sided t-test is a statistical test to determine whether the mean values for two population samples are different. For example, the test can be used to determine whether the percentage of people who experienced a security issue with an IoT device was different for 18-24 year olds and over 65s. If the difference in sample means is statistically significant, it provides strong evidence that the underlying means in the two populations are also different.

[7] Additional details on how YouGov applies weighting to the sample can be found in the Technical Report.

2 Consumer Internet of Things (IoT)

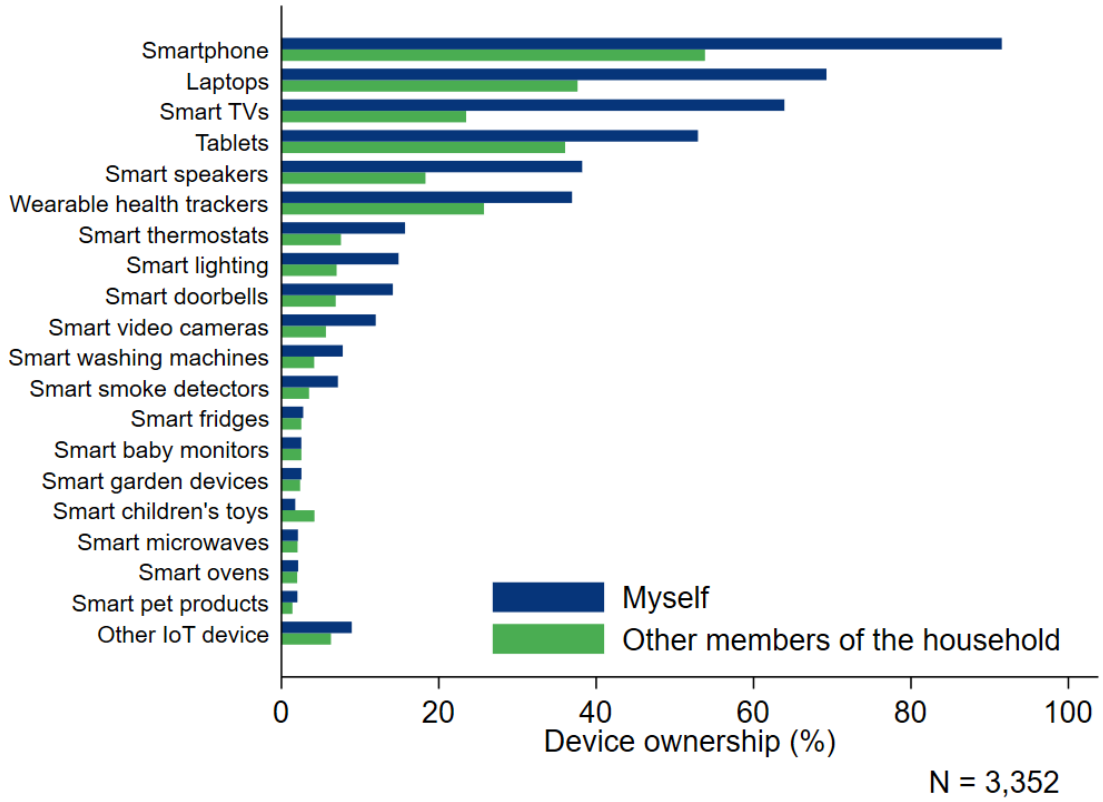
2.1 Consumer IoT device ownership and usage

The first section of the consumer IoT survey explored ownership of different types of consumer IoT devices (Section 2.1.1), the frequency of IoT device usage (Section 2.1.2), and the purpose of usage (Section 2.1.3).

2.1.1 Device ownership amongst individuals and within the household

Consumer ownership patterns vary widely across different IoT devices. The consumer survey explored the proportion of consumers who reported that either they or another member of the household owned different consumer IoT devices. As shown in Figure 1, personal ownership was highest for smartphones (92%), followed by laptops (69%) and smart TVs (64%). Personal ownership of other devices was less common. For example, fewer than 2% of respondents owned a connected children's toy, smart oven or microwave or a smart pet product.

Figure 1 Personal and household ownership of consumer IoT devices (%)



Note: The above figure shows the percentage of survey respondents who responded that either they, or another member of their household, owned a given consumer IoT device. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Across all device types, except connected children's toys, more survey respondents answered that they owned the device themselves as opposed to other members of the household. This finding may reflect the fact that survey respondents may be more likely to own a given IoT device than other members of their household if, for example, they have children. Alternatively, the lower frequency

of ownership for other members of the household may reflect recall difficulty on behalf of respondents. The underlying data for Figure 1 can be found in Annex 4.

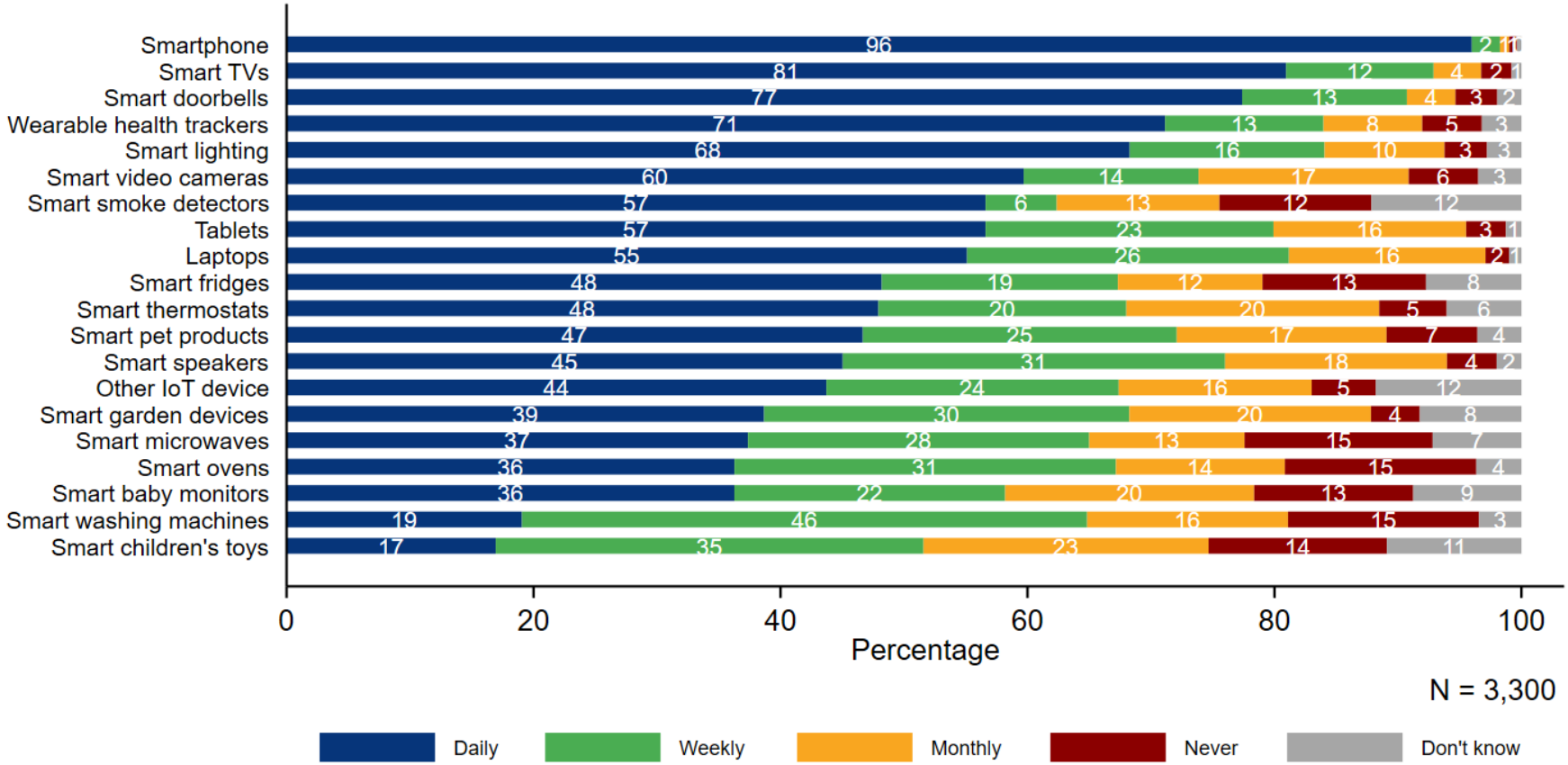
Consumer IoT device ownership by household income

Ownership of different IoT devices varied by household income. Across most device types, personal ownership was higher in higher income households. For example, households earning over £100,000 a year were more likely to own smart kitchen appliances such as smart fridges, smart ovens, and smart microwaves than any other demographic group. Households earning less than £25,000 a year were less likely to own a smartphone than any other income group (9% of people in this group did not own a smartphone).

2.1.2 Frequency of usage for different consumer IoT devices

For devices such as smartphones, smart TVs, or smart doorbells, most respondents indicated that they used these devices daily; 96% of respondents reported using their smartphone every day, and 81% reported using their smart TV every day (Figure 2). Across all devices, over 50% of survey respondents reported using the device at least weekly. The device types with the lowest usage included smart baby monitors and connected children's toys.

Figure 2 Frequency of consumer IoT device usage, by device type



Note: The above figure shows the distribution of frequency of usage across different consumer IoT devices. Each coloured bar represents the percentage of survey respondents who responded that they used the given device at each frequency. The chart uses the weighted sample base.

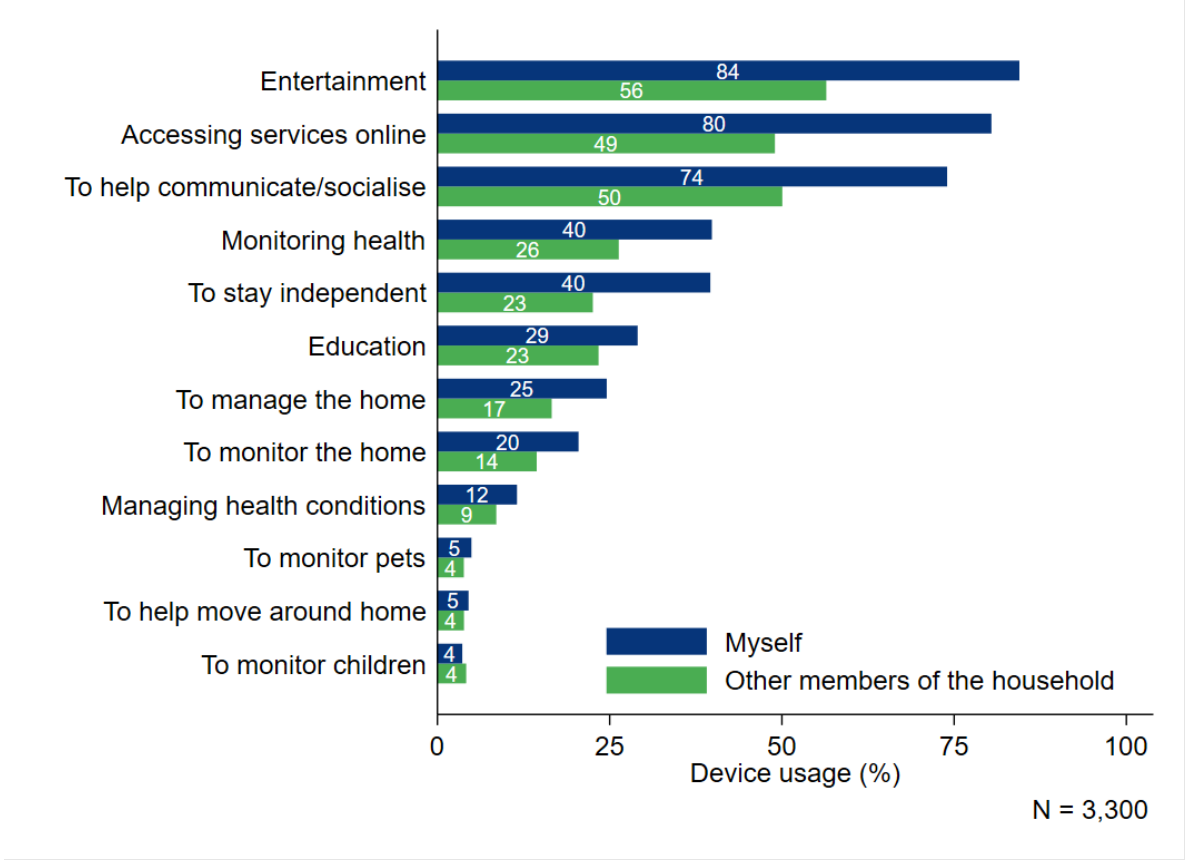
Source: London Economics/YouGov

2.1.3 Purpose of usage for consumer IoT devices

Survey respondents were asked to identify which purposes they used their consumer IoT devices for. Respondents reported that the most popular uses of IoT devices were entertainment (85%), accessing services online (80%), and to help communicate or socialise (74%) (Figure 3).

As with device ownership, across all usage types except monitoring children, a higher share of respondents stated that they themselves used consumer IoT devices for a given purpose than other members of their household. This finding may reflect uncertainty amongst survey respondents about how other members of the household used IoT devices.

Figure 3 Personal and household usage of IoT devices, by purpose (%)



Note: The figure above shows the percentage of survey respondents who indicated that they or another member of their household used consumer IoT devices for the specified purpose. The figure uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Demographic differences in consumer IoT device usage

The purpose of device usage varied by age of respondent. Generally, 18-24 year olds reported higher usage for activities related to entertainment and education relative to older age groups. Younger people were also more likely to use IoT devices to monitor health conditions compared to older age groups. For example, 20% of 25-34 year olds used IoT devices to manage heath conditions, compared to 15% of over 65s.

Consumer IoT device usage by household income

Higher income households were more likely to report using consumer IoT devices than lower income households. For example, 53% of respondents from households with an annual income exceeding £100,000 reported using consumer IoT devices to monitor health, while only 22% of those with an annual household income of than £25,000 a year used consumer IoT devices for the same is purpose.

This finding may reflect the fact that higher income households may be more likely to own IoT devices such as health trackers than lower income households and can therefore use IoT devices for a wider range of purposes. However, the overall ranking of usage purposes was similar across all household income levels.

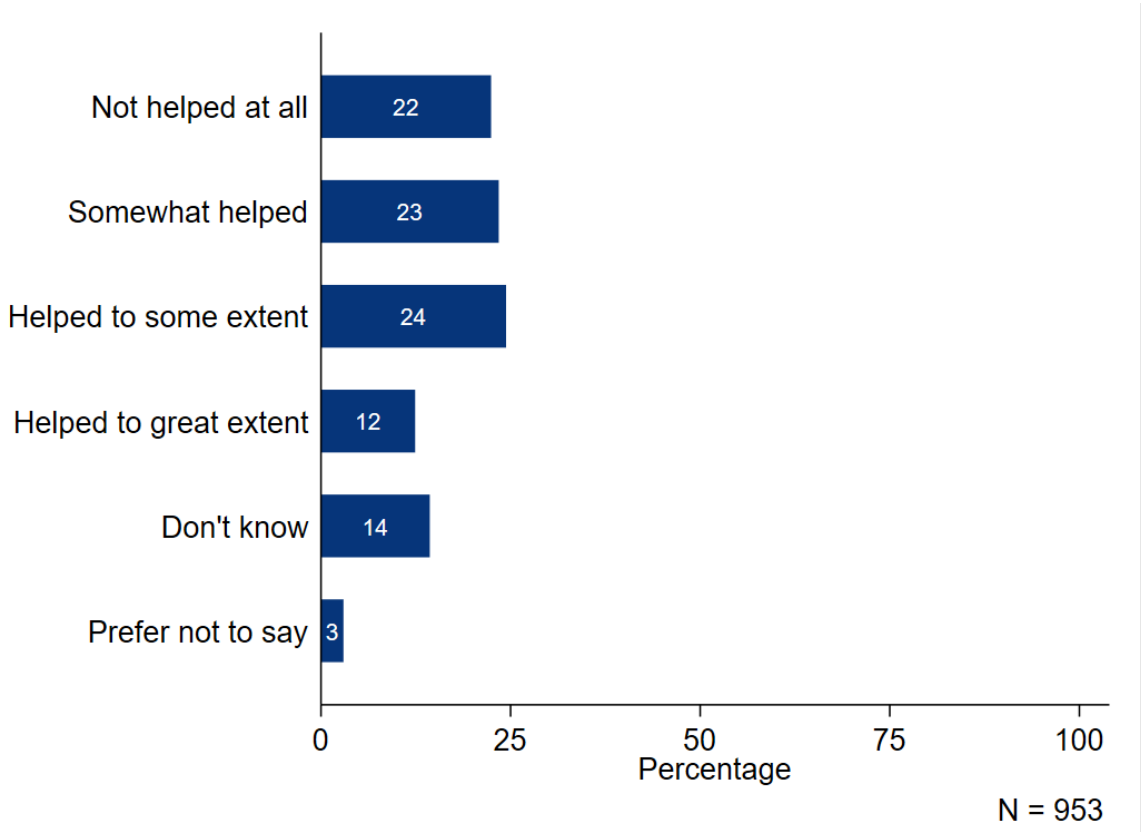
Consumer IoT device usage and disability

The use of consumer IoT devices as a means of accessing and engaging with health services has received increasing emphasis over recent years. For example, a 2022 policy paper published by the Department for Health and Social Care emphasised the need to expand usage of the digital NHS App (accessed via personal IoT devices such as smartphones or laptops) to act as a 'front door' to wider NHS services.[8] The move towards digital engagement with health services is particularly relevant for people who use (or would potentially use) IoT devices to manage health conditions.

Survey respondents who reported having a disability which limited their day-to-day activities were asked to state the extent to which consumer IoT devices had helped them to manage their health conditions. Figure 4 shows that 60% of respondents who had a disability felt that consumer IoT devices had helped to manage their condition at least to some extent, while 22% reported that consumer IoT devices had not helped at all in managing their health condition.

[8] Department of Health and Social Care (2022) A plan for digital health and social care

Figure 4 Extent to which IoT devices have helped with day-to-day management of disability, amongst people who reported having a disability



Note: The percentages in the above figure are calculated based on the sample of respondents who indicated that their day-to-day life was 'limited a little' or 'limited a lot' by a disability. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

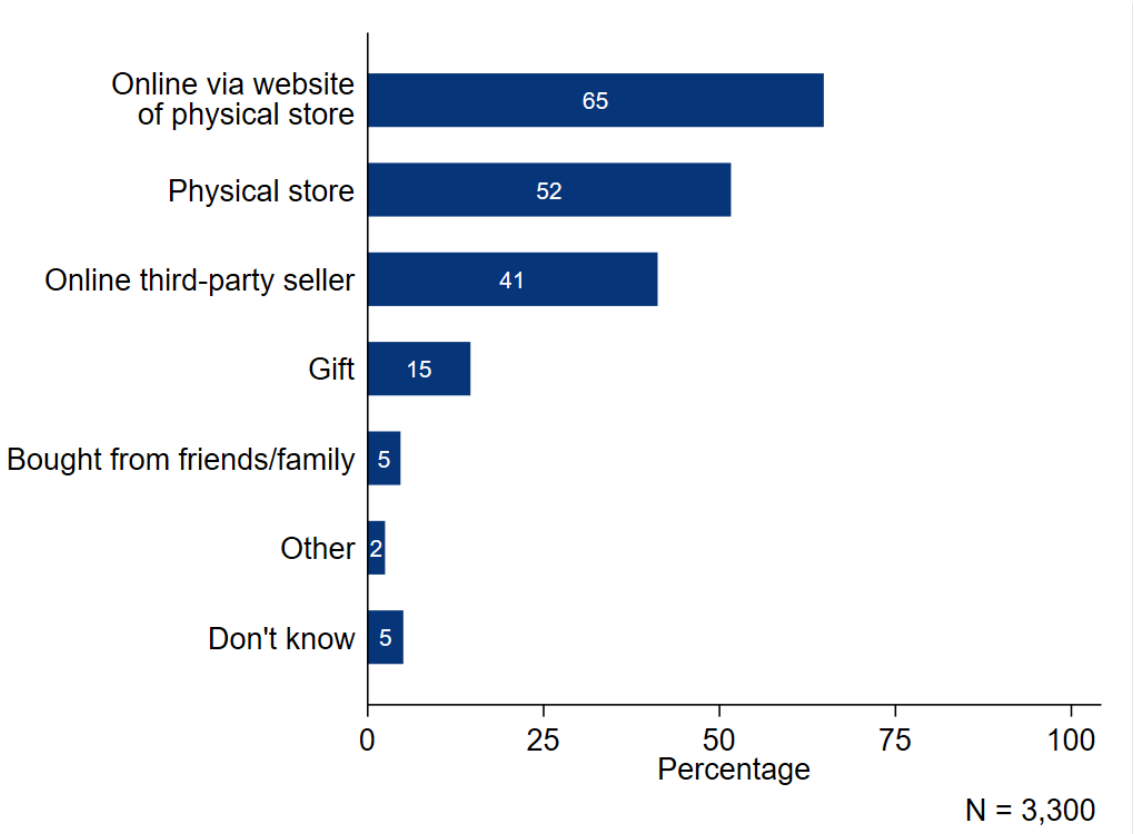
2.2 Purchasing behaviours of consumer IoT devices

The next section of the survey examined consumer purchasing behaviours around IoT devices. Specifically, respondents were asked about the different modes they used to purchase IoT devices (Section 2.2.1), the frequency with which they upgraded, replaced, or disposed of their IoT devices, and to what extent they considered the environmental impact of their IoT devices when doing so (Section 2.2.2).

2.2.1 Mode of IoT device purchase

The survey examined purchasing behaviours relating to consumer IoT devices. The most popular modes of purchasing consumer IoT devices were online via the website of a physical store (65%), in a physical store (52%), and through an online reseller or marketplace (41%) (Figure 5).

Figure 5 Percentage of consumers using different modes of device purchase



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Demographic differences in consumer IoT device purchasing behaviour

Younger people were more likely to report purchasing devices online through the website of a physical store. For example, 73% of 18-24 year olds had purchased a consumer IoT device online through the website of a physical store. By contrast, only around 50% of over 65s had purchased a consumer IoT device using the same method. Purchasing directly from a physical store was most popular with older respondents, with around 60% of over 65s reporting that they had purchased an IoT device directly through a physical store.

Respondents with a lower household income were less likely to report purchasing an IoT device online through the website of a physical store. Amongst respondents with an annual household income of less than £25,000, 54% had purchased an IoT device online through the website of a physical store, compared to 80% of people with an annual household income greater than £50,000.

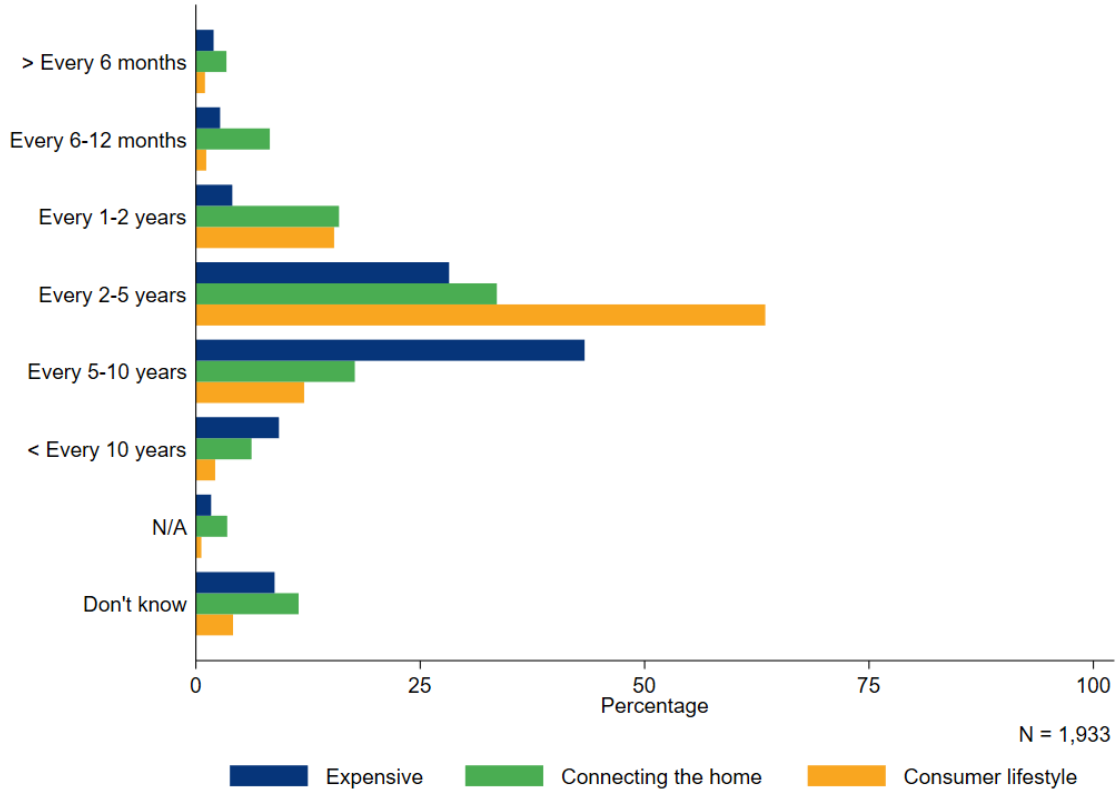
2.2.2 Upgrading, replacing, or disposing of Consumer IoT devices

Survey respondents who had previous experience upgrading, replacing, or disposing of a consumer IoT device, were asked how frequently they carried out these activities.

'Expensive' IoT devices such as smart TVs or smart fridges, were replaced less frequently than 'connecting the home' devices such as smart speakers or lightbulbs, and 'consumer lifestyle' devices including smartphones or smart watches (Figure 6). Around 50% of respondents reported that they upgraded, replaced, or disposed of expensive IoT devices every 5-10 years or more infrequently. Around 80% of respondents indicated that they upgraded, replaced, or disposed of consumer

lifestyle IoT devices every 2-5 years or more frequently. The underlying data for Figure 6 is provided in Annex 5.

Figure 6 Frequency of upgrading, replacing, or disposing of consumer IoT device, by device group



Note: The figure above displays the percentage of survey respondents indicating that they replaced, disposed, or threw away their IoT devices with the following frequency. The results are shown separately for three different groups of IoT device – 'Expensive', 'connecting the home', and 'consumer lifestyle'. This question was shown only to survey respondents who had experience replacing their IoT devices. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

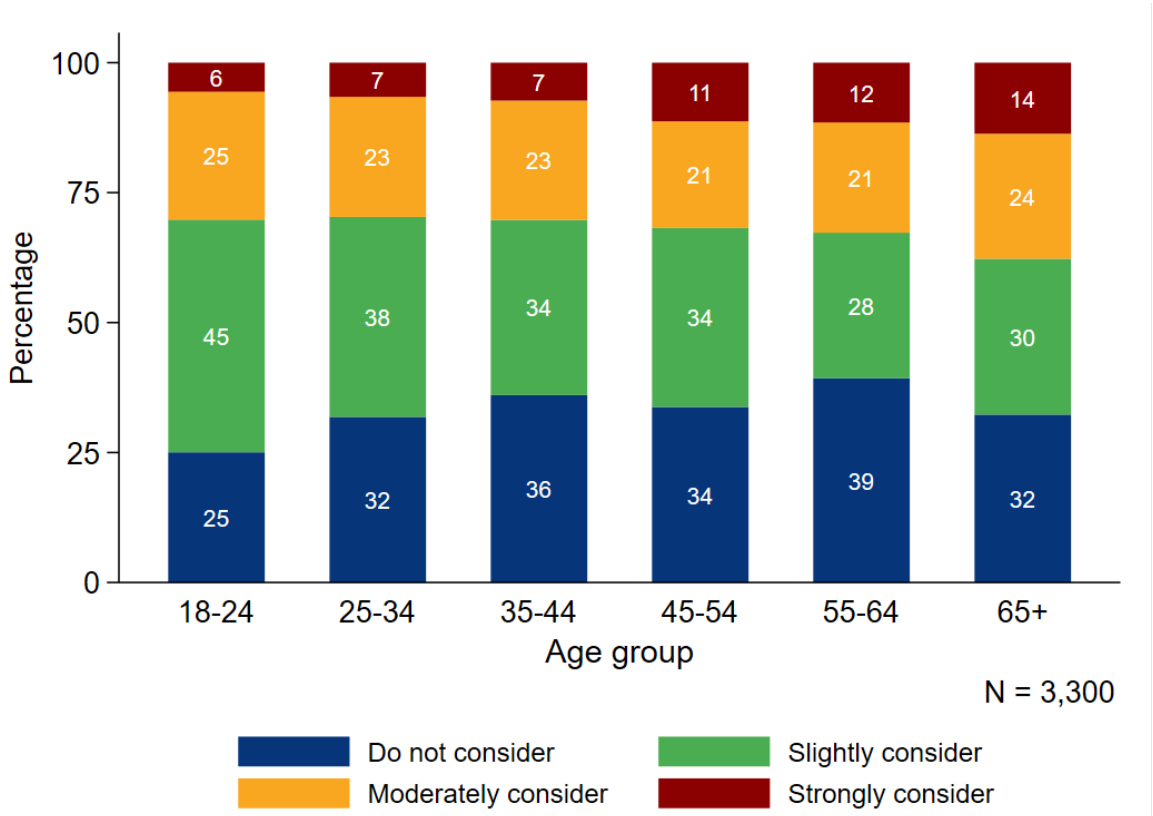
Source: London Economics/YouGov

The environmental impact of buying, replacing, or disposing of consumer IoT devices

When buying, replacing, or disposing of a consumer IoT device, 67% of respondents reported that they slightly considered the environmental impact, with 32% either moderately or strongly considering the environmental impact (Figure 7). Around one-third of respondents indicated that they did not consider the environmental impact at all when buying, replacing, or disposing of a consumer IoT device.

Older people exhibited stronger attitudes towards the environmental impact of buying, replacing, or disposing of consumer IoT devices. Respondents in the over 65 age group were most likely to report strongly considering the environmental impact of buying, replacing, or disposing of their devices (14%), compared to 6% of 18-24 year olds. However, older respondents were also more likely to report not considering the environmental impact of buying, replacing, or disposing of their devices at all. Respondents in the 18-24 year old age group were least likely to report not considering the environmental impact at all.

Figure 7 Extent to which consumers consider environmental impact when buying, replacing, or disposing of IoT devices, by age group



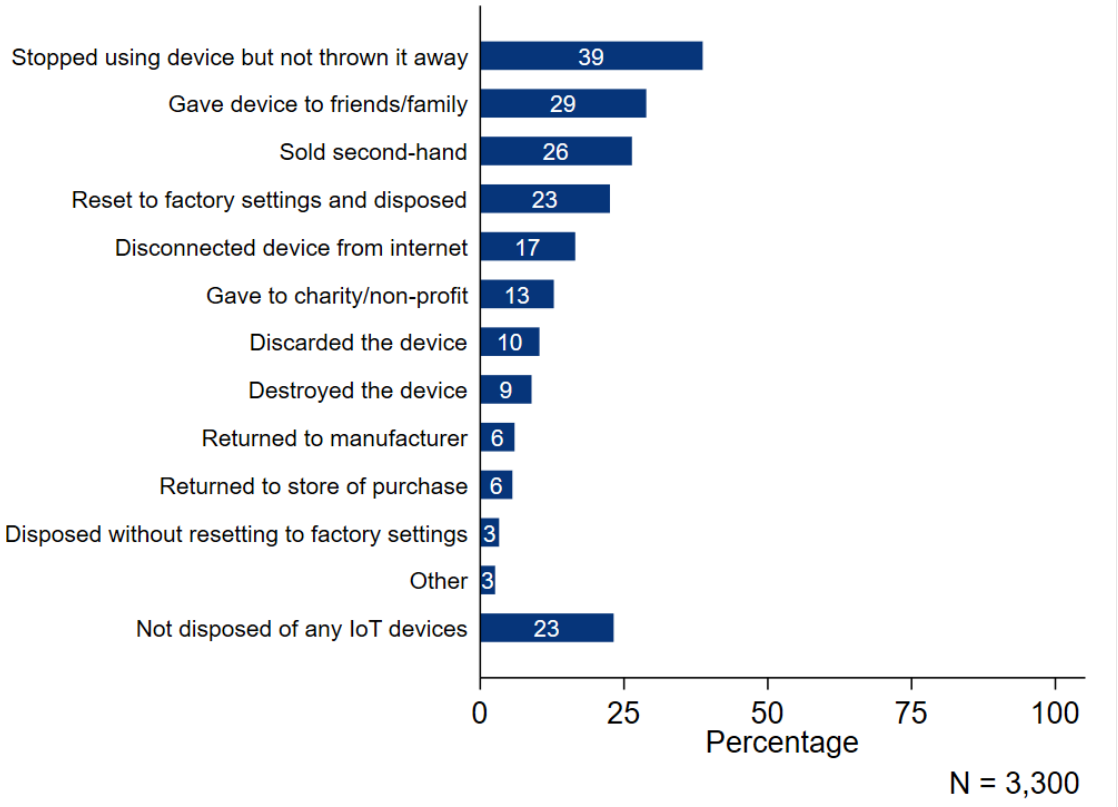
Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Methods for disposing of consumer IoT devices

The most popular method by which respondents reported disposing of their IoT devices was to stop using the device but not to dispose of it (39%) (Figure 8). The second and third most popular methods of device disposal were passing the device to friends and family (29%) and selling the device second-hand (26%). Just under a quarter of survey respondents said that they had not disposed of any IoT devices (23.2%).

Figure 8 Proportion of consumers using different methods to dispose of IoT devices



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: YouGov/London Economics survey

2.3 Consumer attitudes towards IoT device security

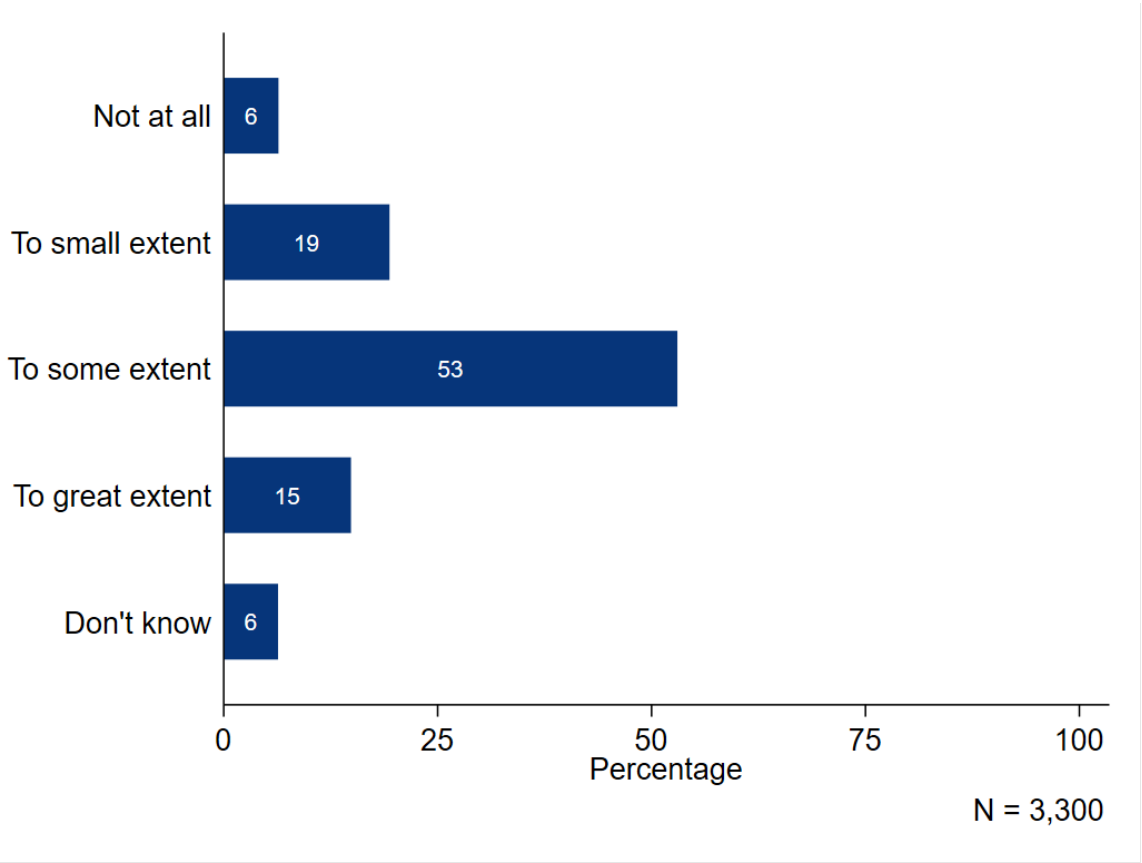
The survey looked at consumer attitudes towards IoT device security. Section 2.3.1 examines consumer trust in the security of their IoT devices, Section 2.3.2 explores consumer attitudes around the accessibility of security and privacy information for IoT devices, whilst Section 2.3.3 examines consumer attitudes around the relative responsibility of retailers and manufacturers for consumer IoT device security.

2.3.1 Consumer trust in security of IoT devices

Most survey respondents indicated that they trust the security of their IoT devices at least to a small extent (87%) (Figure 9). Only 6% of respondents said that they did not trust the security of their IoT devices at all, and 6% responded that they 'don't know'.

Higher-income households were more likely to trust the security of their devices. Among households earning more than £100,000 per year, 23% of respondents said they trusted the security of their IoT devices 'to a great extent', compared to 13% in households earning less than £25,000 per year.

Figure 9 Extent to which consumers trust security of IoT devices



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

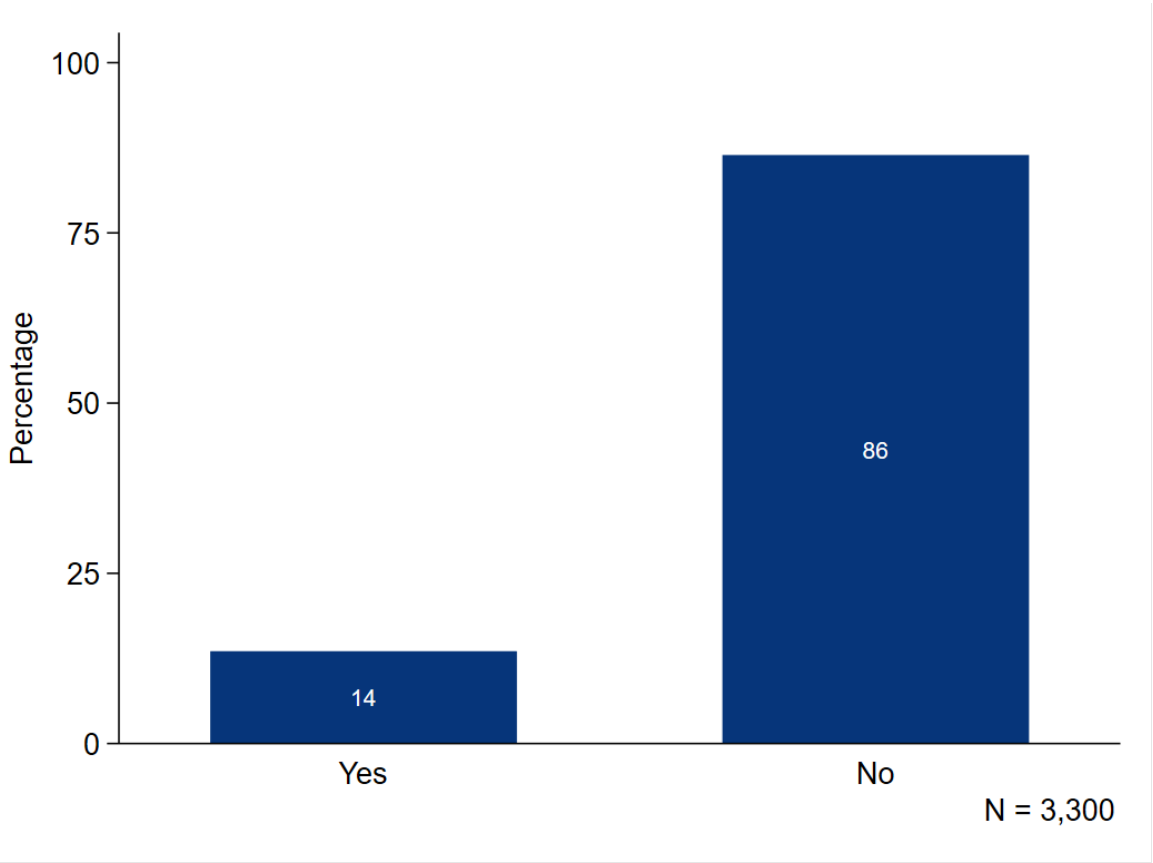
Source: London Economics/YouGov

2.3.2 Accessibility of security and privacy information

The following section explores consumer perceptions regarding the accessibility of security and privacy information on IoT devices. Specifically, survey respondents were asked whether they knew the minimum support period for their consumer IoT devices and where they expected to find security information for their device(s).

Most respondents (86%) did not know the minimum support period for their IoT devices (Figure 10). Households with an annual income of over £100,000 were more likely to know the minimum support period for their devices (19%) than households with an annual income of less than £25,000 (12%).

Figure 10 Percentage of respondents who know the minimum support period for their IoT devices

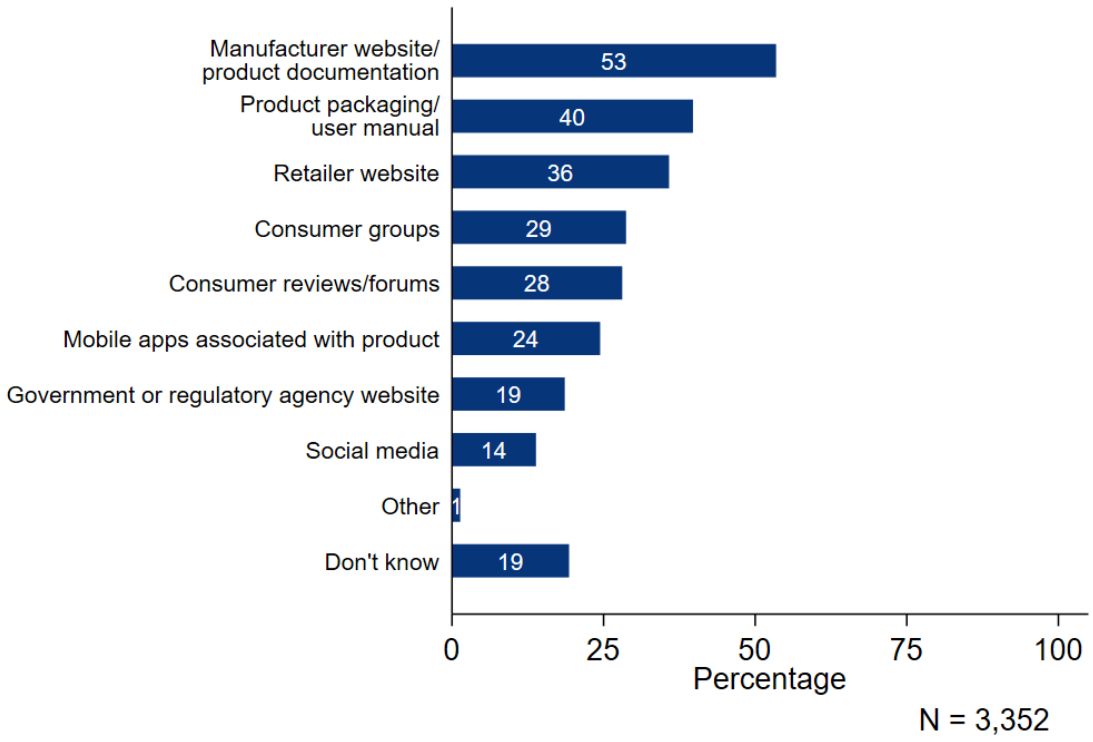


Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

The most common locations where respondents expected to find security information were on the manufacturer website or in product documentation (53%), product packaging or user manuals (40%), and retailer websites (36%) (Figure 11). Around one in five respondents stated that they did not know where they would expect to find security information for their IoT devices, this was higher for women and amongst respondents with a lower level of education.

Figure 11 Percentage of respondents who reported expecting to find security information for their IoT devices in different locations



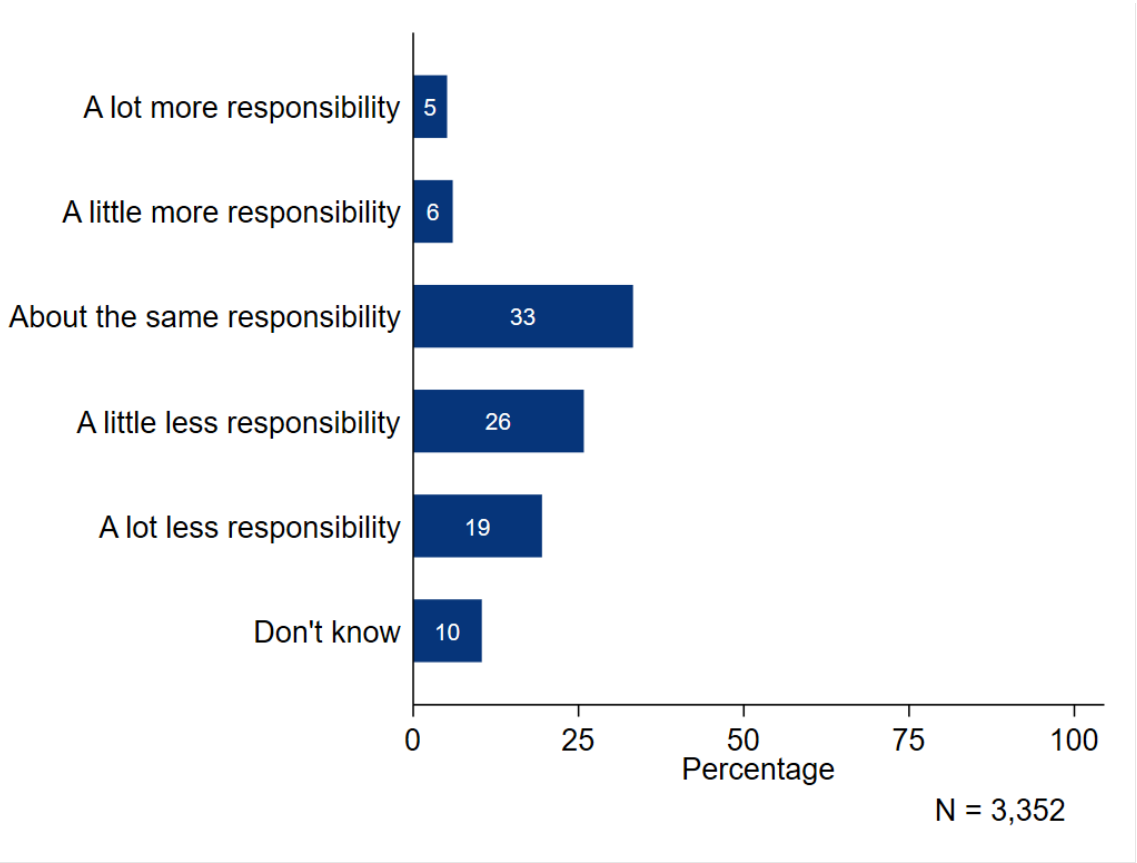
Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

2.3.3 Responsibility of manufacturers and retailers for product safety and security

The survey asked respondents to state whether they felt retailers had more, less, or about the same responsibility for IoT product safety and security than manufacturers. The results suggest that respondents generally felt that manufacturers had more responsibility for product safety and security than retailers (Figure 12). Only 11% of respondents felt that retailers had 'a little more' or 'a lot more' responsibility for product safety and security than manufacturers, while a larger proportion (45%) felt that retailers had 'a little less' or 'a lot less' responsibility.

Figure 12 Extent to which respondents felt retailers had more/less responsibility for IoT device safety and security than manufacturers



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

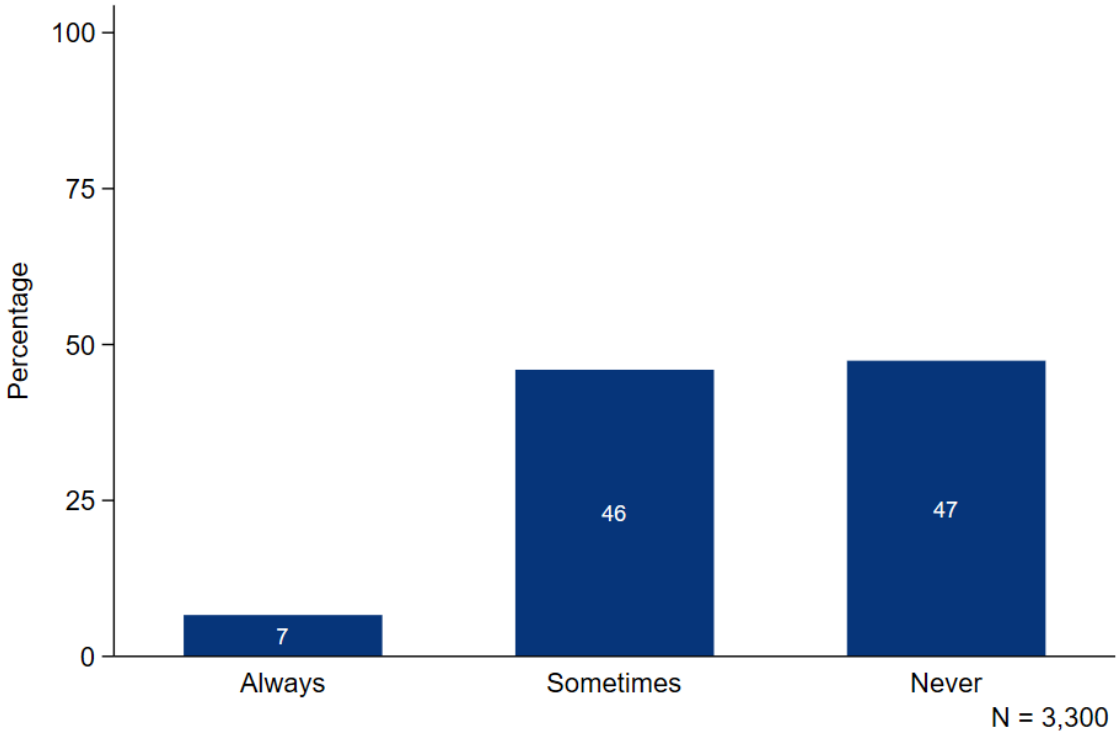
2.4 Consumer behaviours towards device security

In addition to exploring consumer attitudes towards the security of their IoT devices, the survey asked respondents about their behaviours towards device security. Survey respondents were asked whether they switched off the internet connectivity of their IoT devices (Section 2.4.1), the extent to which they considered security as a factor when purchasing IoT devices (Section 2.4.2), and their willingness to pay for improved device security (Section 2.4.3).

2.4.1 Switching off device internet connectivity

Slightly over a half (53%) of respondents indicated that they switched off the internet connectivity of their consumer IoT devices at least some of the time. Around 7% of respondents said they always switched off the internet connectivity of their IoT devices (Figure 13).

Figure 13 Frequency with which respondents switched off IoT device internet connectivity

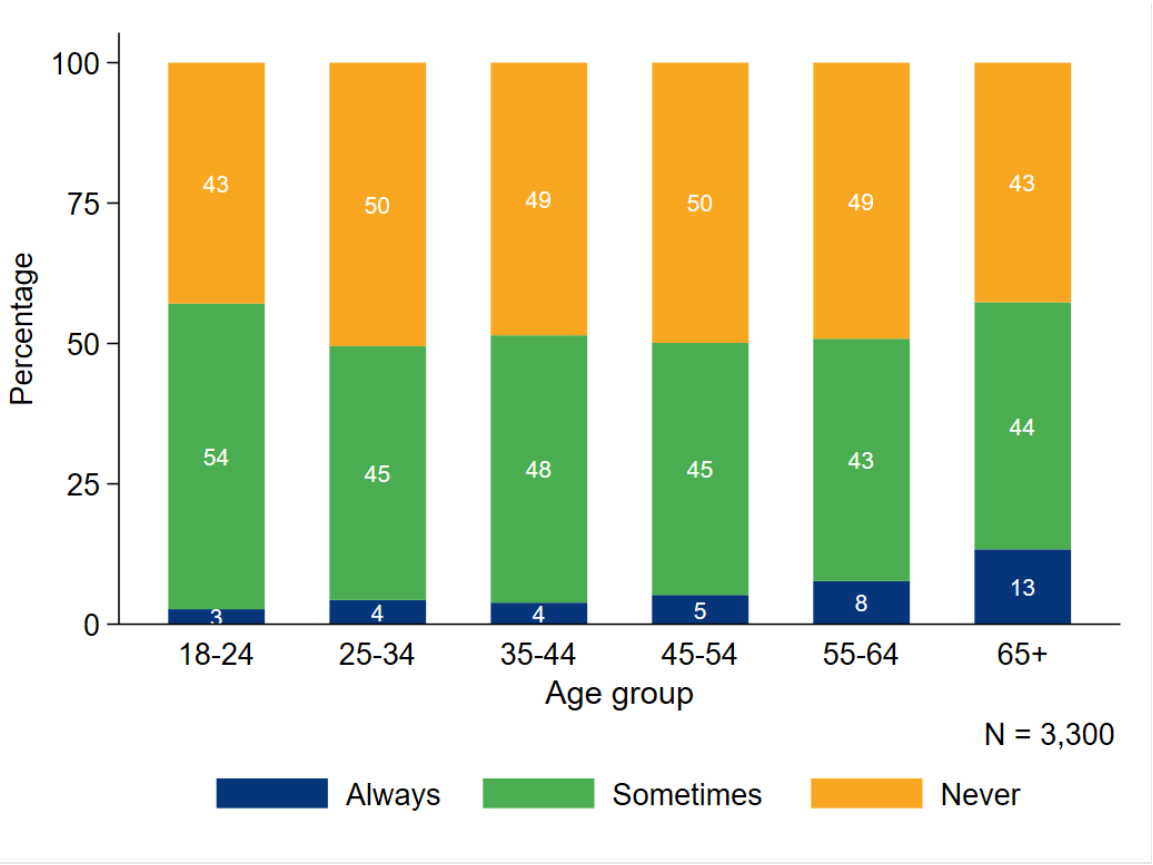


Source: London Economics/YouGov

Demographic differences in switching off internet connectivity of consumer IoT devices

Behaviours around switching off the internet connectivity of consumer IoT devices varied with age (Figure 14). Respondents over the age of 65 were around four times more likely to say they 'always' switch off the internet connectivity of their IoT device than respondents aged 18-24 (13% of over 65s always turned off their device's internet connectivity, compared to 3% of 18-24 year olds).

Figure 14 Frequency with which respondents switched off IoT device internet connectivity, by age group



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

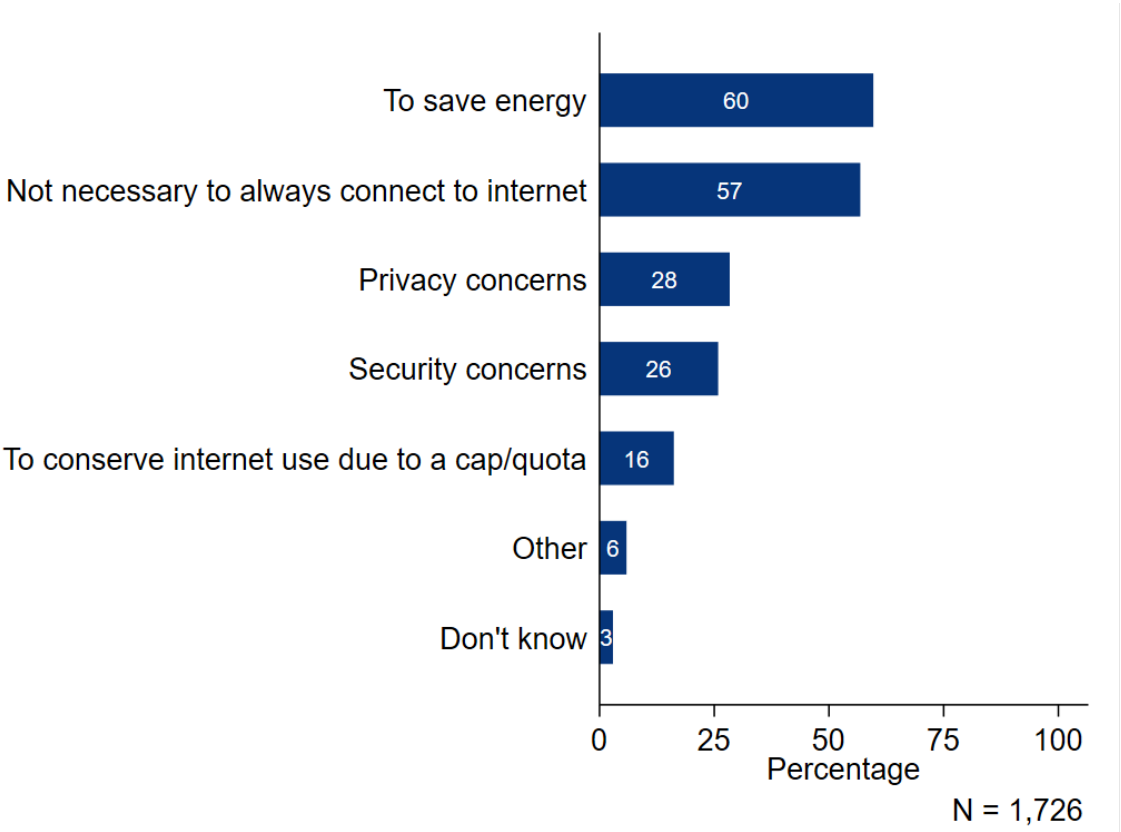
Source: London Economics/YouGov

Reasons for switching off internet connectivity of consumer IoT devices

Survey respondents who reported switching off their IoT device connectivity at least sometimes were asked to state the reasons for doing so. The most cited reasons for switching off device connectivity were to save energy (60%) and that it is not necessary to connect the device to the internet all the time (57%) (Figure 15).

Concerns over privacy and security were less-commonly stated but still important reasons for switching off connectivity, with 28% and 26% of respondents citing these reasons respectively. Men were more likely to report turning off their device connectivity due to security concerns than women (30% of men gave security concerns as a reason for switching off device connectivity, compared to 22% of women).

Figure 15 Reasons for switching off IoT device internet connectivity, among those who did switch off internet connectivity (% of respondents)



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

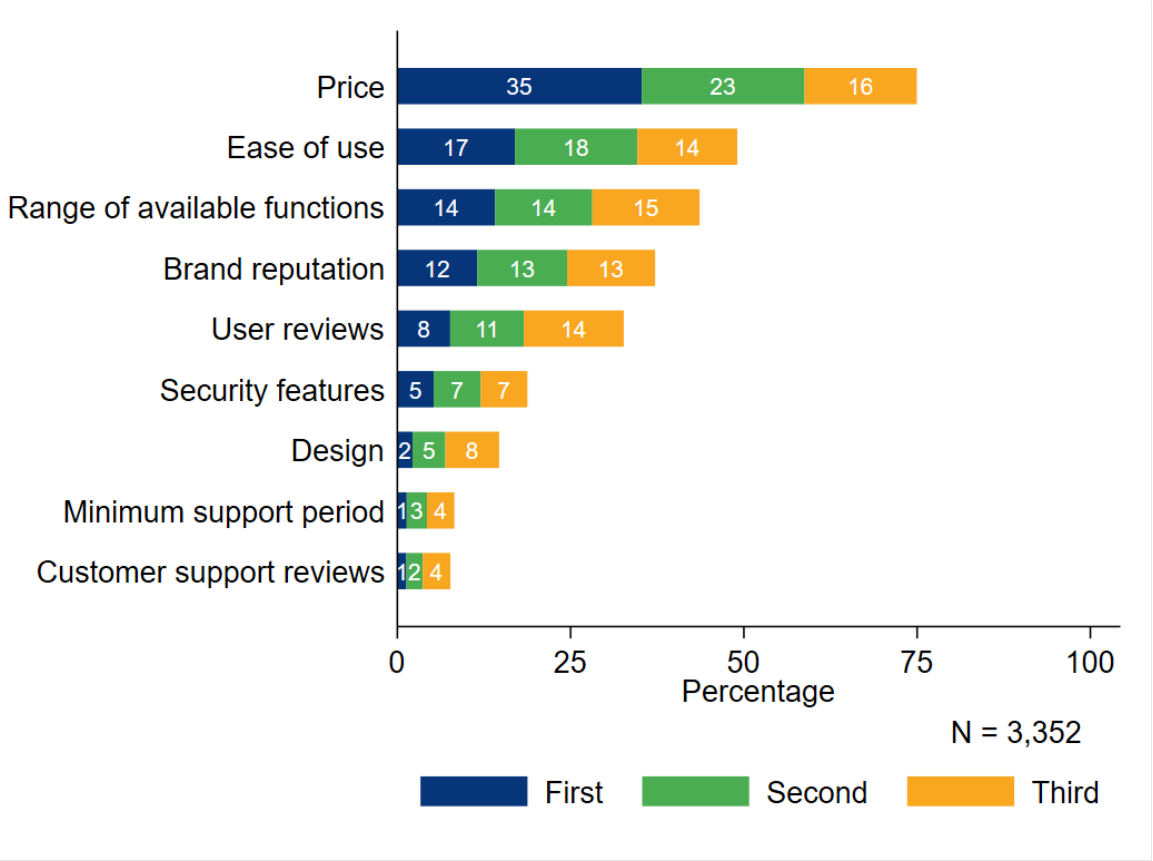
Source: London Economics/YouGov

2.4.2 The extent to which consumers consider security when buying consumer IoT devices

Respondents were asked to rank the top three product features that are most important to them when purchasing an IoT device. The survey responses suggest that price is the most important characteristic to consumers (Figure 16). Around 75% of respondents ranked price as one of their top three characteristics, with 35% indicating that price was the most important characteristic.

Other important characteristics included the functionality of the device (ease of use and range of available functions). Security features and the minimum support period were reported to be less important to respondents, with 19% ranking security features in their top three features and 8% reporting the minimum support period in their top three features.

Figure 16 Percentage of survey respondents ranking each product characteristic as top three most important when purchasing IoT devices



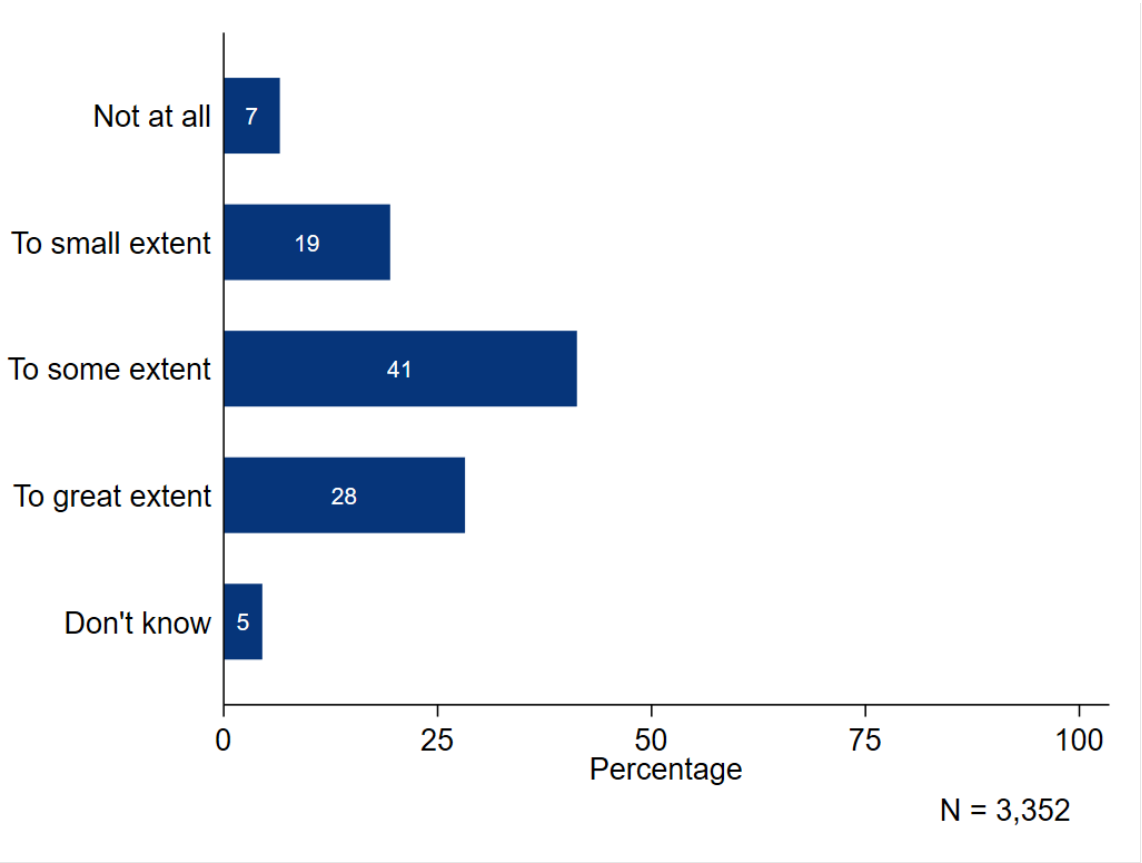
Note: Each coloured bar represents the percentage of survey respondents ranking each device characteristic in the stated position (first, second, or third). Respondents were asked to select the top three product characteristics they would consider when purchasing consumer IoT devices. The total height of each bar represents the percentage of respondents selecting the given characteristic in their top three most important product characteristics. Percentages are calculated based on the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Respondents were directly asked the extent to which they consider security when purchasing an IoT device (Figure 17). The results suggest that most respondents reported that they considered the security of IoT devices to some extent (69%). Around 25% of respondents indicated that they considered security to a small extent or not at all.

Together, the findings from Figure 16 and Figure 17 suggest that security is considered to some extent when purchasing an IoT device, however it is less important to respondents in their purchasing decision compared to price, functionality and reputation of the product and brand. Older respondents were more likely to report that they consider the security of a device 'to a great extent' (33% of over 65s) compared to 23% of 18-24 year olds.

Figure 17 Extent to which consumers consider security when buying IoT devices



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

2.4.3 Consumer willingness to pay a price premium for enhanced device security

The results presented above suggest that most people consider the security of consumer IoT devices to some extent, but that overall price is the most important characteristic for many consumers in their purchasing decision.

To explore whether consumers are willing to pay more for enhanced device security, survey respondents were asked to state the percentage premium they would be willing to pay for improvements in cyber security when purchasing an IoT device. Specifically, respondents were asked to state the percentage premium they would be willing to pay for an IoT device in return for a given percentage reduction in the number of security incidents or breaches relating to that device each year.

Respondents were randomly allocated to be shown either a 50% reduction or a 90% reduction in the number of device incidents. Respondents were also asked to estimate their willingness to pay separately for three different types of IoT device: 'expensive' (e.g. smart TVs, smart fridges), 'connecting the home' (e.g. smart speakers, smart lightbulbs), and 'consumer lifestyle' (e.g. smartphones, smart watches).

It should be noted that the willingness to pay questions were not embedded within a full stated preference analysis, as this would have required a separate standalone survey. Therefore, the results in this section should be interpreted with caution.

For 'expensive' and 'connecting the home' IoT devices, around 50% of respondents stated that they would not be willing to pay any premium for a 50% improvement in device security. The corresponding percentage for 'consumer lifestyle' IoT devices was 42%.

There was little variation in the distribution of willingness to pay across the 50% vs. 90% improvement in security (graphs showing the full distribution of willingness to pay are shown in Annex 2 and Annex 3). In both cases, the most frequent response was that respondents were not willing to pay anything more for enhanced device security.

More respondents indicated they would be willing to pay a premium for improvements in the security of 'consumer lifestyle' devices such as smartphones or smart watches. This result may reflect the fact that these devices were more commonly owned and used by survey respondents, so the security of these devices may be considered relatively more important than for less frequently used devices such as smart fridges.

Among the set of 237 survey respondents who reported experiencing a security issue with their IoT device(s), there was evidence of a greater willingness to pay for enhanced device security. A higher proportion of respondents who had experienced a security issue indicated they would be willing to pay a premium for enhanced device security than for the full sample. For example, 69% of respondents indicated that they would be willing to pay a premium for enhanced security of a consumer lifestyle device, compared to 58% in the whole sample.

Average willingness to pay for enhanced consumer IoT device security

Table 2 shows the mean willingness to pay for enhanced consumer IoT device security for the sample of respondents who indicated that they would be willing to pay a premium. Across device types, the mean percentage premium willingness to pay was higher for a 90% improvement in device security than a 50% improvement (Table 2).

The highest mean percentage premium willingness to pay was for consumer lifestyle devices such as smartphones or smart watches. Taking the results for a 90% improvement in device security, there is a statistically significant difference between the mean willingness-to-pay for consumer lifestyle devices compared to both connecting the home devices and expensive devices.[9] Across device types, respondents aged over 45 were more likely to indicate that they would be willing to pay a premium for enhanced device security.

Table 2 Mean willingness to pay (percentage premium) for enhanced security, by IoT device

IoT device type	50% improvement in security	90% improvement in security
Expensive	18%	19%
Connecting the home	17%	19%
Consumer lifestyle	22%	24%

Source: London Economics/YouGov

Actions taken instead of paying extra for enhanced consumer IoT device security

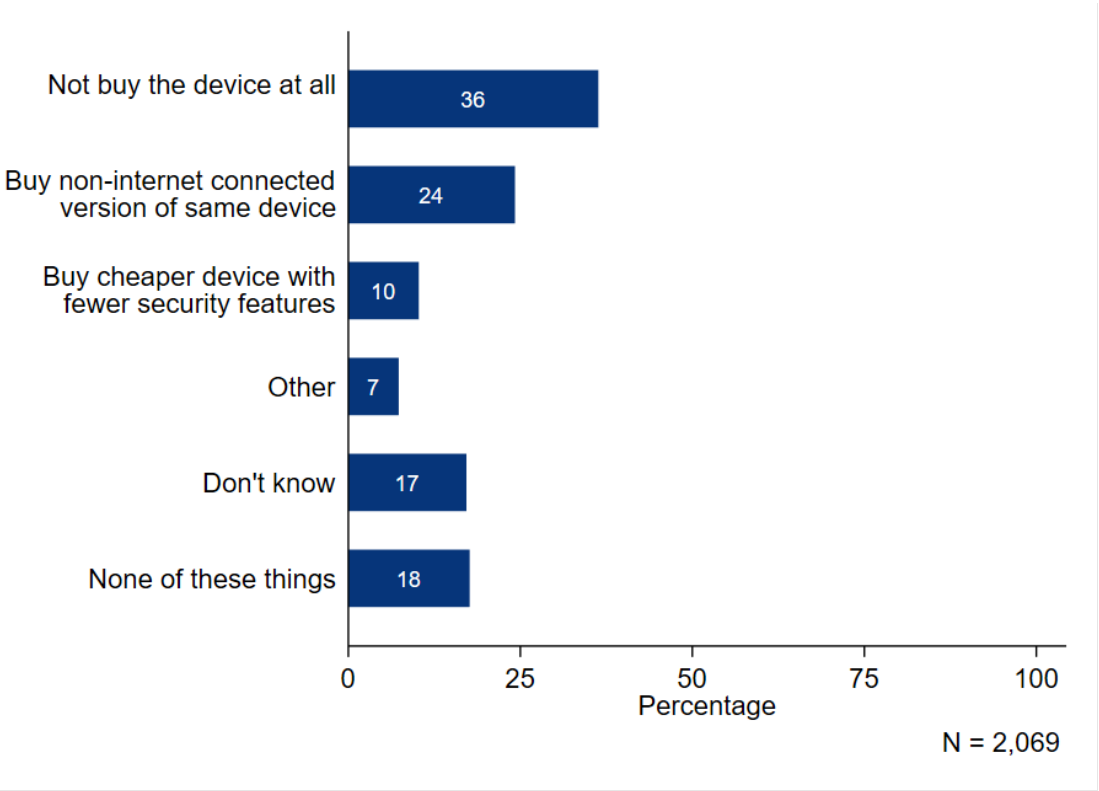
The results presented in the previous section demonstrate that around half of survey respondents were not willing to pay anything more for enhanced consumer IoT device security. Survey

[9] The null hypothesis is rejected at the 95% significance level. For consumer lifestyle vs. connecting the home devices the associated p-value was 0.0464, and for consumer lifestyle vs. expensive devices the p-value was 0.0016.

respondents who indicated that they would not be willing to pay anything more for enhanced security were asked what alternative actions they would take instead.

Around a third of respondents (36%) said that they would not buy a device at all instead of paying more for improved security, while around a quarter (24%) indicated that they would buy a non-internet connected version of the same device (Figure 18). The possibility of buying a non-internet connected device depends on the device type – for some types of device such as smart kitchen devices, consumers may be more able to switch to non-internet connected appliances instead of paying more for improved security compared to a smartphone. Respondents seemed less willing to purchase a cheaper IoT device that was connected, but with fewer security features (10%).

Figure 18 Percentage of respondents who indicated they would take alternative actions instead of paying more for improved IoT device security, among those who did not want to pay extra for enhanced device security



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

2.5 Consumer IoT cyber security issues

The IoT survey examined consumer-reported experiences of cyber security issues to do with their IoT devices. Specifically, Section 2.5.1 details the extent to which consumers had experienced cyber security issues with their IoT devices, Section 2.5.2 details the key impacts arising from experiencing an issue, and Section 2.5.3 details the behaviours undertaken by respondents having experienced a cyber security issue with their IoT device(s).

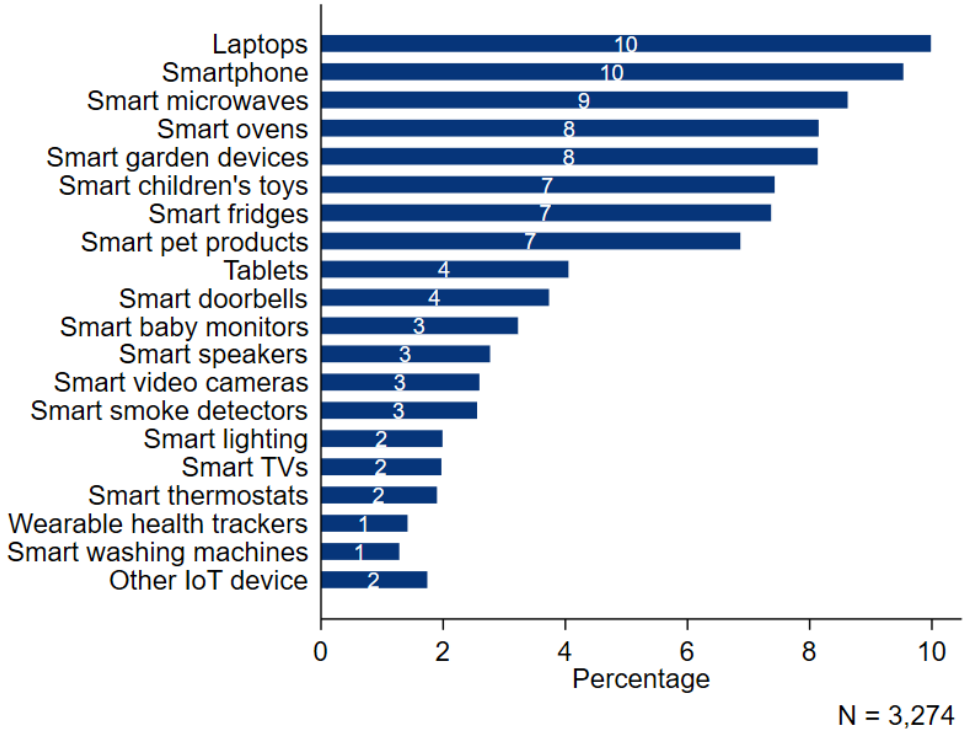
2.5.1 Experiences of cyber security issues

The survey included questions related to respondents' experience with cyber security issues affecting their IoT devices. Figure 19 shows the percentage of survey respondents who stated that

they had experienced a security issue by different consumer IoT device types. Each bar represents the percentage of respondents who owned a given device personally and reported experiencing a security issue relating to that device.

The most prevalent devices for security issues were laptops (10%) and smartphones (9.5%). Since these items are also the most commonly owned consumer IoT devices, they make up a large share of the total number of devices subject to security issues. Smart kitchen devices such as smart microwaves, ovens, and fridges ranked highly in terms of the proportion of users who experienced security issues with these devices. Most survey respondents (84%) indicated that they were not aware of experiencing any security issues with their consumer IoT devices. Men were more likely to report experiencing an IoT device security issue than women – 19% of male respondents reported experiencing at least one security issue, compared with 14% of female respondents.

Figure 19 Percentage of respondents experiencing security issue, by device type



Note: The figure above shows the percentage of survey respondents who indicated that they had experienced a security issue or issues with the given device. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Consumers reporting experiencing security issues with multiple devices

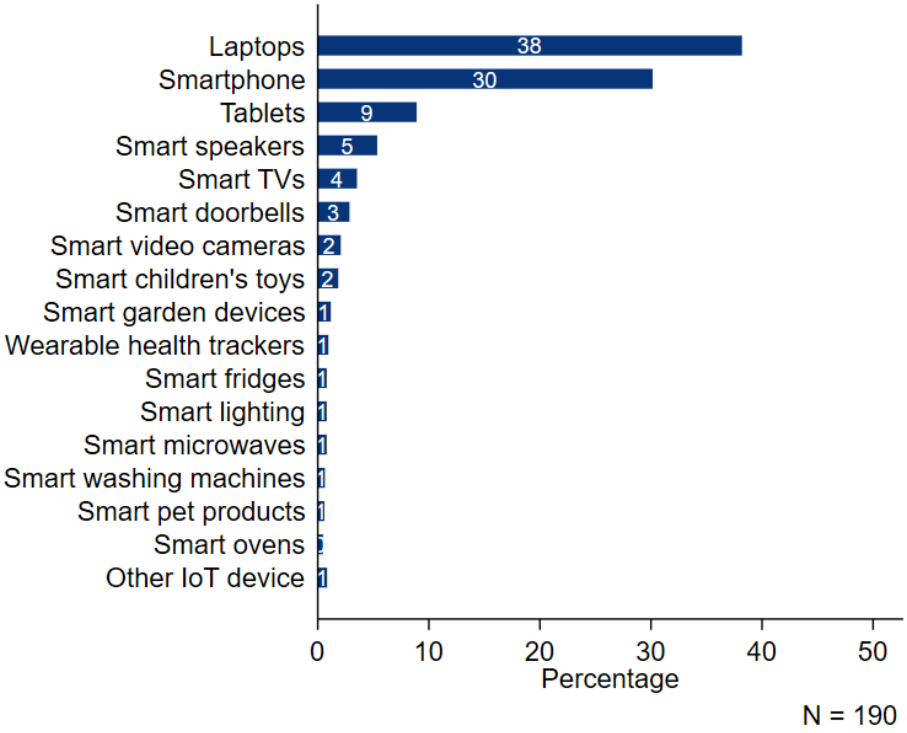
Around 6% of respondents (190) reported experiencing a security issue with more than one consumer IoT device. These respondents were asked to identify which of the devices had caused them the most concern due to a security issue. The devices most commonly cited as causing the most concern due to a security issue were laptops (38%) and smartphones (30%) (Figure 20).

Different types of issues experienced with consumer IoT devices

Respondents who reported experiencing security issues with their IoT devices were asked about the type of security issue. Among respondents who had experienced a security issue, the most common types of security issue were receiving a security notification from the IoT device (64%) or the device

being subject to malware or viruses (55%). There was some variation in the type of security experienced by age group. For example, over 65s were less likely to report being victim to malware or a virus (41%) compared to any other age group.

Figure 20 Devices that caused respondents most concern due to a security issue (% of respondents)



Note: The above chart shows the percentage of survey respondents indicating that each IoT device type had given them the most concern due to a security issue, among the subset of respondents who experienced security issues with more than one IoT device. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

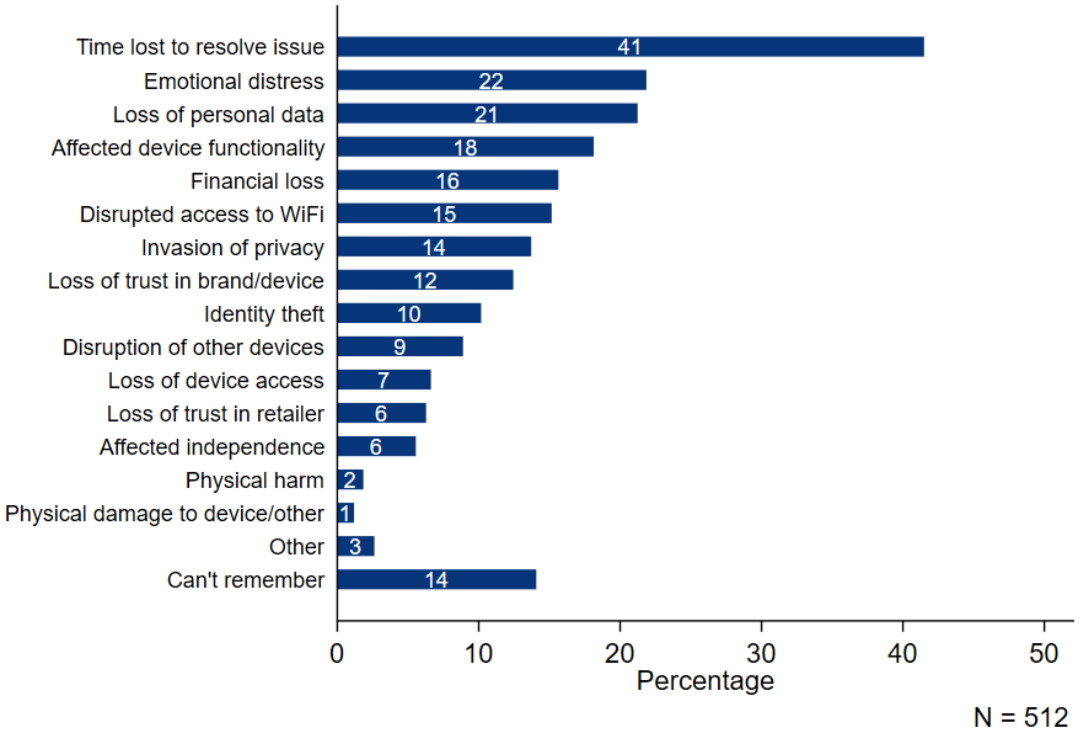
Source: London Economics/YouGov

2.5.2 Impacts of cyber security issues

Being victim of cyber security issues can have multiple impacts, including emotional impacts such as stress or anxiety, financial loss, and loss of trust in IoT devices. In the survey, respondents who reported that they had experienced a security issue with their IoT device were asked to identify which of the different potential impacts they had experienced due to their security issue.

The most prevalent impact of experiencing a security issue was time lost in resolving the issue (41%), followed by emotional distress (22%) (Figure 21). Other common impacts included functional impacts such as loss of personal data (21%), changes to device functionality (18%), and financial loss (16%). People who had a disability were twice as likely to report losing trust in the brand or IoT device following a security issue (19%) than people without a disability (9%).

Figure 21 Percentage of consumers experiencing impact following security issues with IoT devices



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

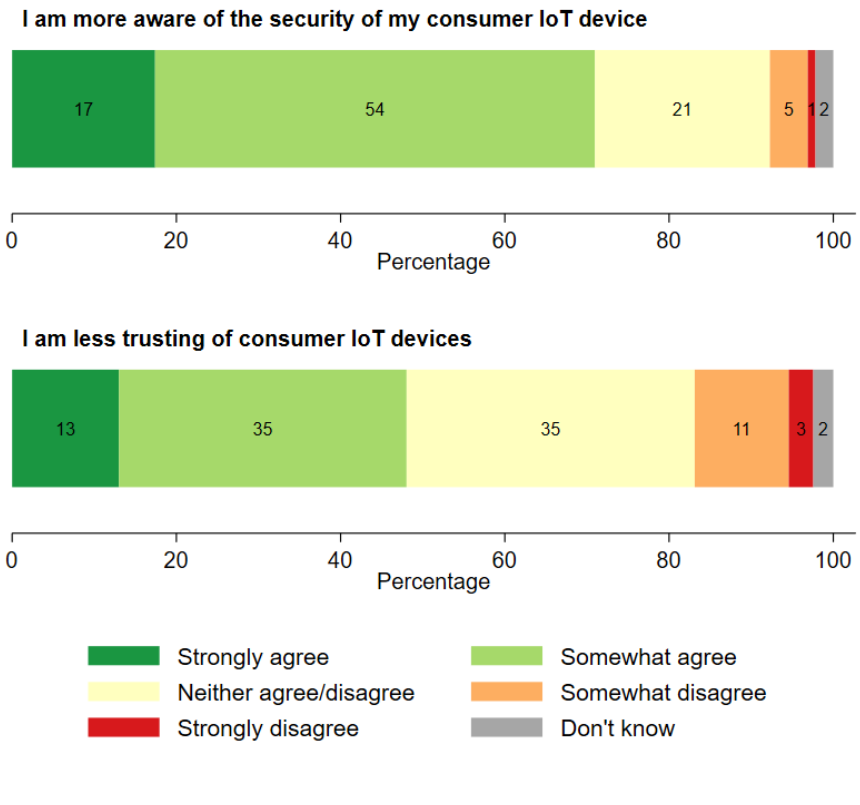
Changes in attitudes towards consumer IoT device security following a security issue

In addition to specifying the type of impacts they had suffered due to device security issues, respondents were asked the extent to which they agreed with statements regarding how their attitudes to device security changed following experiencing a security issue. The statements were:

- "I am more aware of the security of my consumer IoT device."
- "I am less trusting of consumer IoT devices."

The results suggest that attitudes towards consumer IoT devices change after experiencing a security issue (Figure 22). Nearly three quarters (71%) of respondents said that they strongly or somewhat agreed that they were more aware of the security of their consumer IoT device following a security issue. However, there was a weaker relationship between experiencing an issue and subsequent loss of trust in IoT devices. Around half (48%) of respondents who reported experiencing a security issue strongly or somewhat agreed that they were less trusting of consumer IoT devices.

Figure 22 Changes in consumer attitudes regarding security following a security issue



Note: The chart uses the weighted sample base.

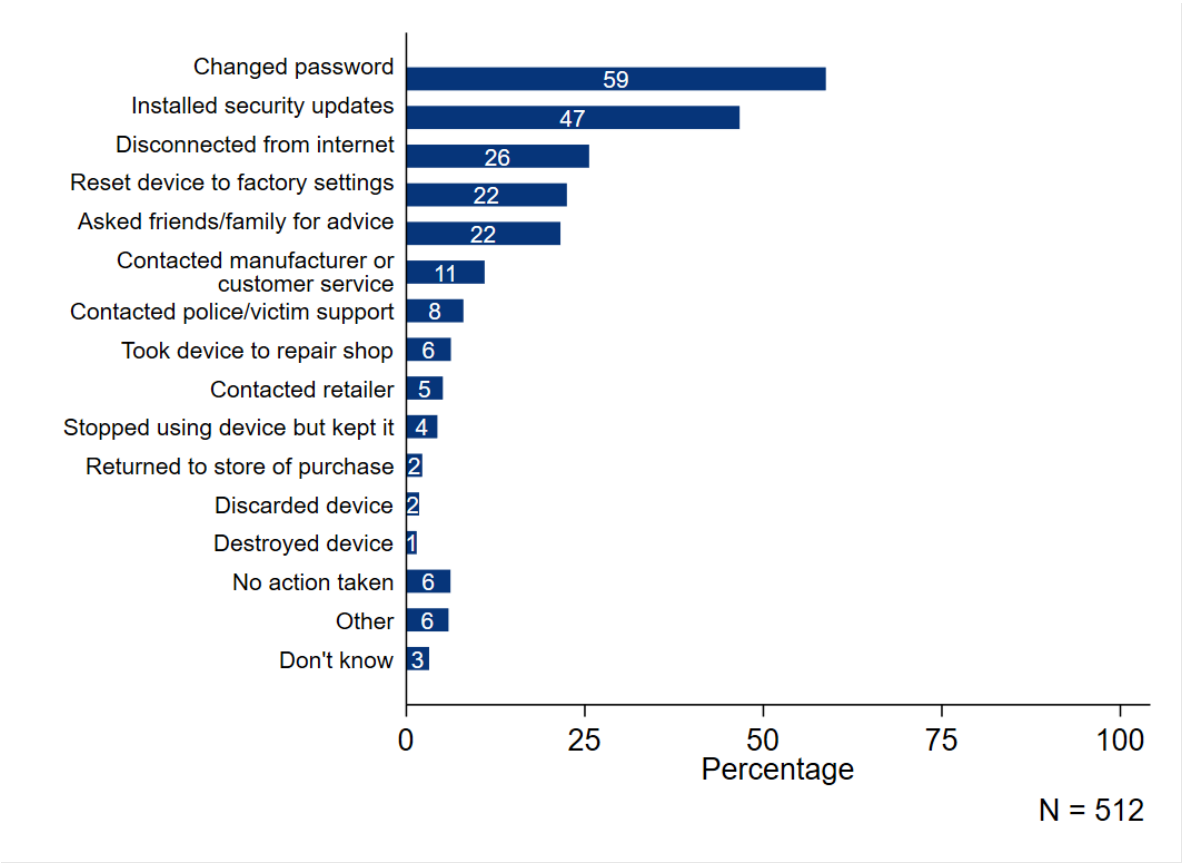
Source: London Economics/YouGov

2.5.3 Behaviours following cyber security issues

Respondents who had reported experiencing cyber security issues with their IoT device were asked about their behaviour following the incident. The most common actions taken were changing the device password (59%), installing device security updates (47%), and disconnecting the device from the internet (26%) (Figure 23).

Only 6% of respondents indicated that they had taken no action in response to the security issue. However, respondents in lower income households were more likely to report not taking any action – 12% of respondents in households earning less than £25,000 per year reported taking no action following a security issue.

Figure 23 Percentage of respondents who took different actions following a consumer IoT device security issue

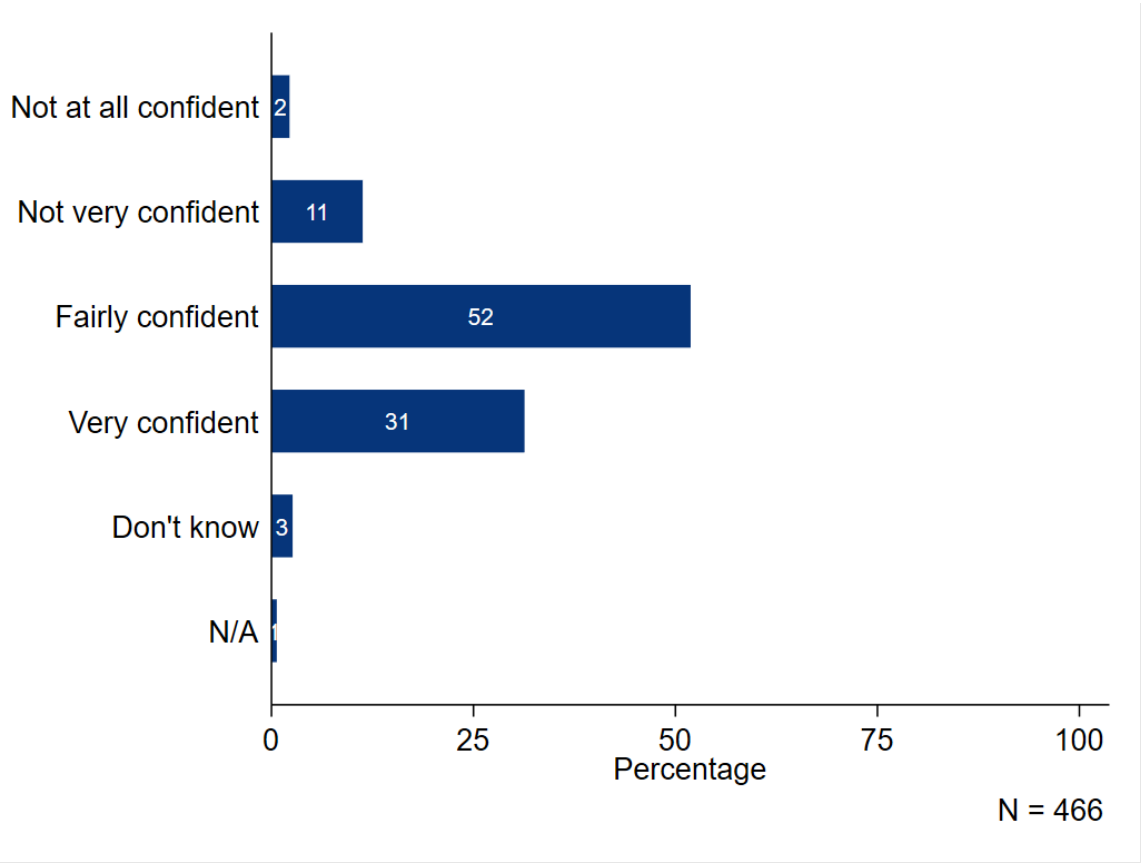


Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Survey respondents indicated a relatively high degree of confidence that the action(s) they had taken had resolved the security issue(s) they had experienced (Figure 24). Most respondents were either fairly confident (52%) or very confident (31%) that the action they had taken had resolved the security issue. Around 13% of respondents stated that they were not at all or not very confident that the action taken had resolved the security issue.

Figure 24 Extent to which respondents are confident that the action taken resolved the security issues



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

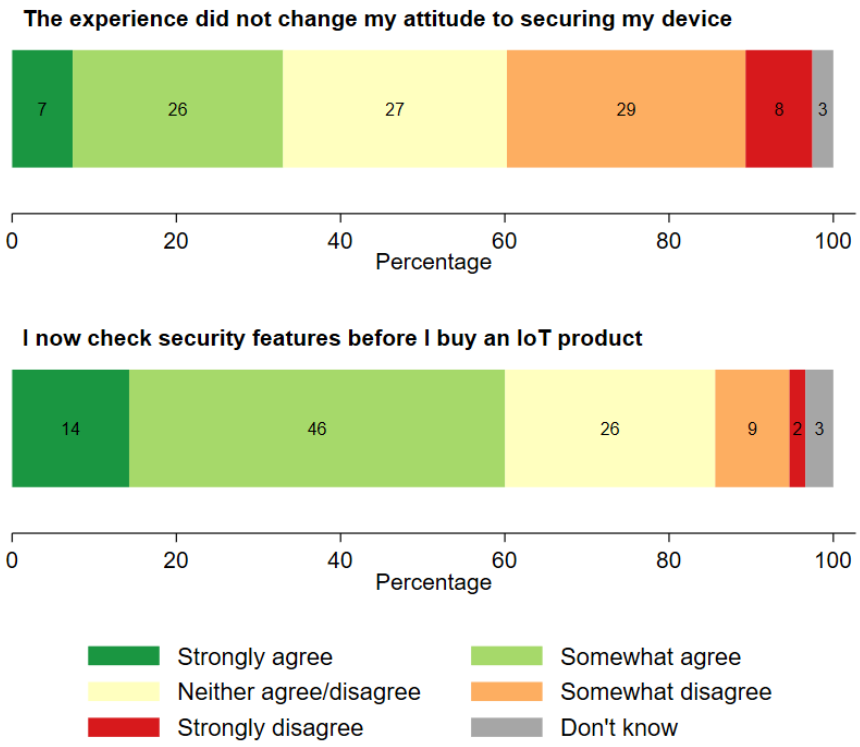
Changes in behaviour towards consumer IoT device security following a security issue

Respondents were asked to state the extent to which they agreed or disagreed with statements regarding changes in behaviour following an IoT device security issue. The statements provided were:

- "The experience did not change my attitude to securing my device."
- "I now check or consider security features before I buy / use an IoT product."
- "I do not buy / use IoT devices anymore."
- "I have taken steps to improve the security of my IoT device."

The responses to the first two statements are displayed in Figure 25. The chart in the upper panel shows that around one-third of respondents agreed that the security issue had not changed their attitude towards securing their IoT device. A similar proportion (37%) disagreed with the statement, implying that they had changed their attitude towards device security. The chart in the bottom panel shows that a majority (60%) of respondents said that they now checked security features before buying consumer IoT products. This finding indicates that security features are a salient consideration when purchasing IoT products for people who experience security issues.

Figure 25 Changes in consumer behaviour following a device security issue



Note: The chart uses the weighted sample base.

Source: London Economics/YouGov

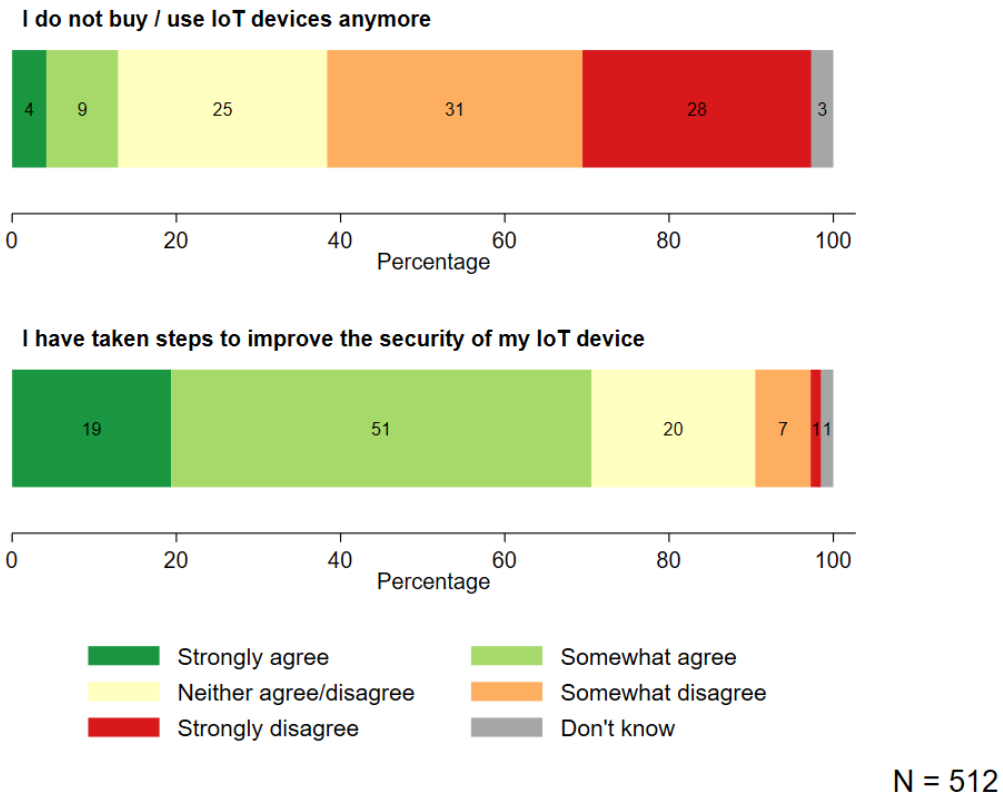
The responses to statements 3 and 4 are shown in Figure 26. The chart in the upper panel shows that only a small percentage of respondents who reported experiencing a security issue agreed or strongly agreed that they stopped buying or using IoT devices (13%). The degree to which people stopped using consumer IoT devices depended on the affected device. For example, 85% of people who had an issue with a smart washing machine responded that they did not buy or use IoT devices anymore, compared to just 10% for people who had an issue with a smartphone.

This disparity reflects the fact that some types of IoT technology such as smartphones or laptops are more embedded into daily life, and users may find it more difficult to switch away from these devices relative to devices like smart kitchen technology. In addition, for some IoT devices such as smart fridges it is easier to switch to a non-connected version of the device compared to devices such as smartphones or laptops. Respondents may have interpreted this question in terms of the specific device(s) they had an issue with, as opposed to in terms of their usage of consumer IoT devices more generally.

The chart in the lower panel shows that most respondents took steps to improve the security of their IoT device; 61% strongly or somewhat agreed with the statement, "I have taken steps to improve the security of my IoT device".

Together, these results imply that behavioural change following a consumer IoT device security issue is more commonly expressed by taking practical steps to improve the security of existing IoT devices, as opposed to reducing or stopping use of IoT devices.

Figure 26 Changes in consumer behaviour following a device security issue



Note: The chart uses the weighted sample base.

Source: London Economics/YouGov

3 Apps and app stores

3.1 Consumer device ownership and app store usage

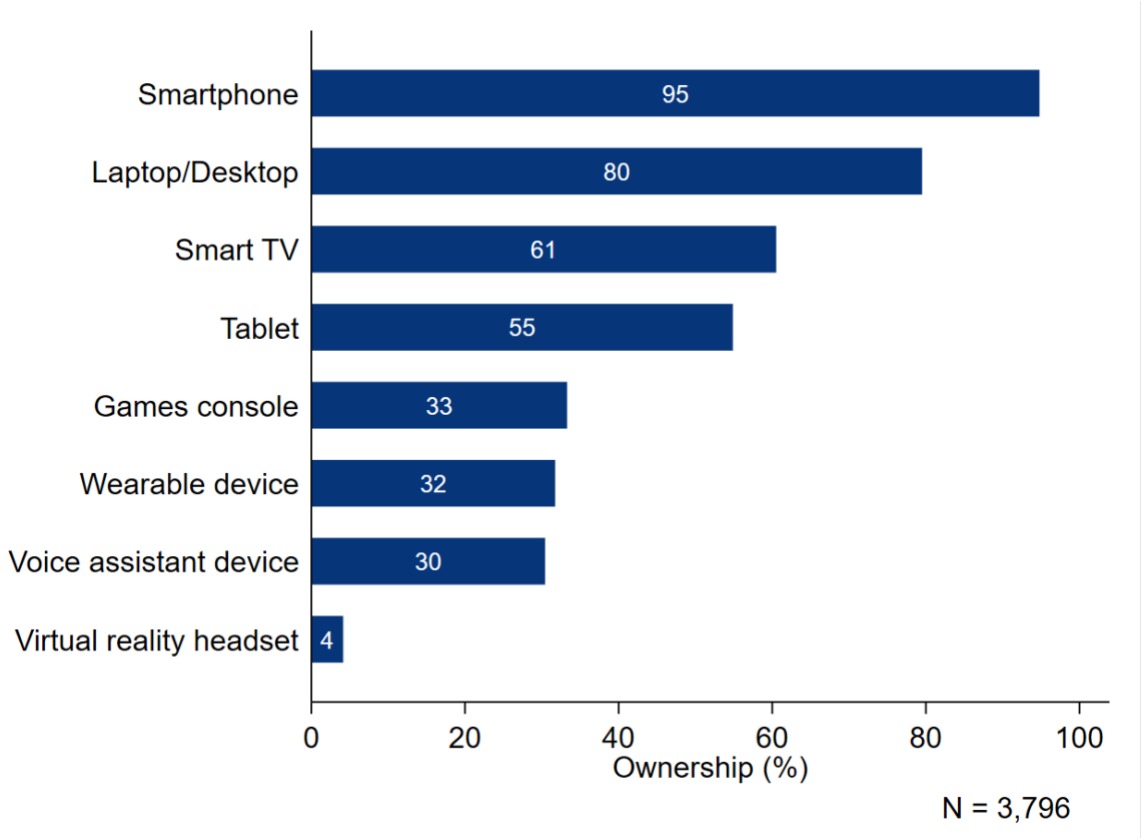
The first section of the apps and app stores survey explored consumer ownership of different devices which use apps and app stores, and the proportion of consumers that use different app stores on these devices.

3.1.1 Consumer ownership of different devices

Survey respondents were asked to identify which devices they personally owned among the list in Figure 27. The results show that the most commonly owned devices were smartphones (95%), laptops or desktops (80%), and smart TVs (61%).

Across most devices (except for smartphones, voice assistant devices, and wearable devices), men reported higher ownership than women. Ownership of different devices generally did not vary widely across different income groups. Lower income groups (where household annual income is less than £25,000) reported lower ownership of smart TVs, games consoles, voice assistant devices, and wearable devices compared to households earning more than £50,000 per year. Respondents who reported that their day-to-day activities are limited by a disability also reported lower ownership of most devices than those who are not limited by a disability.

Figure 27 Personal ownership of different devices (% of respondents)



Note: The above figure shows the percentage of respondents who responded that they owned a given device. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

3.1.2 Consumer usage of app stores

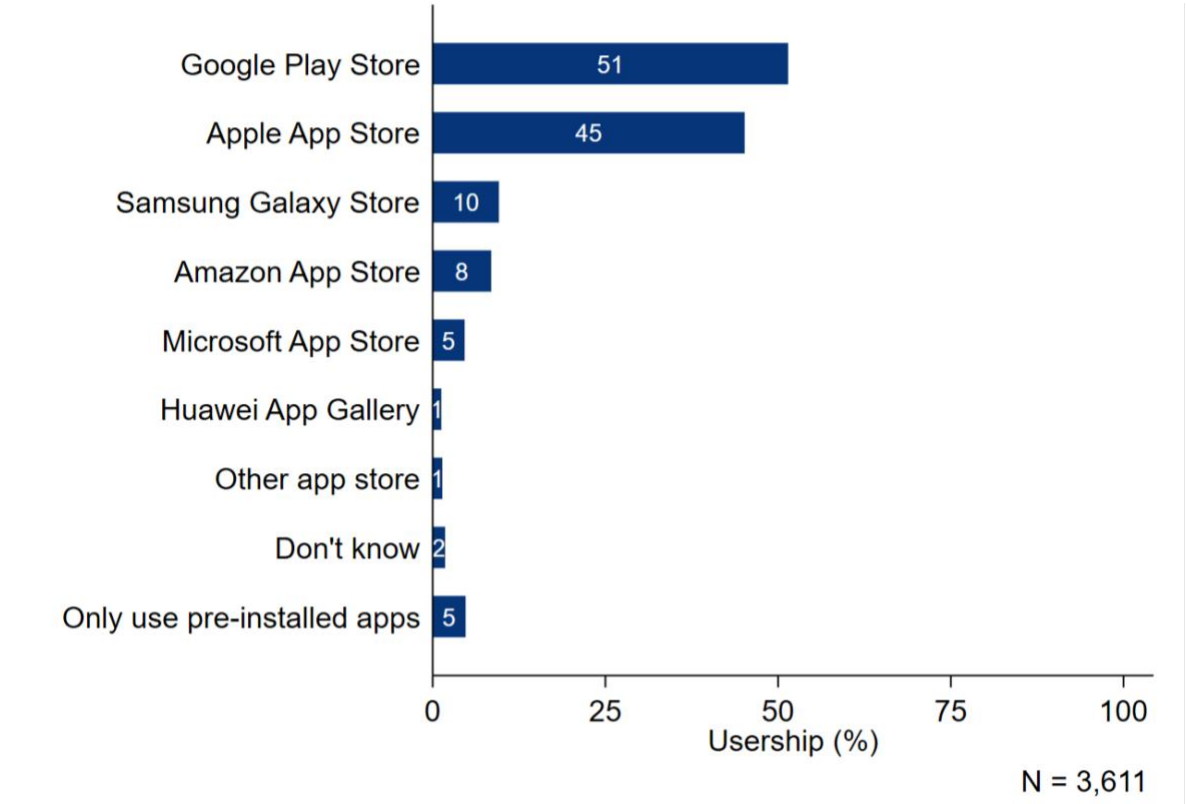
Survey respondents who reported owning a particular device were asked to identify which app stores they used on their device, or if they use only the pre-installed apps that came on the device when it was first purchased (and hence do not use the app store). The results for smartphones, laptops/desktops and smart TVs are presented below. The results for the remaining devices are presented in Annex 1.

Smartphone app store usage

The Google Play Store was the most used app store on smartphones (52%) followed by the Apple App Store (45%) (Figure 28). Apple App Store users were more likely to be female and have a higher household income, whereas the opposite was true for the Google Play Store, where users were more likely to be male and have a lower household income.

Only a small proportion of respondents reported that they only use pre-installed apps on their smartphone (5%). This was higher amongst lower income households (under £25,000) (7%) and those over 65 (14%).

Figure 28 Usage of different smartphone app stores (% of respondents)



Note: The above figure shows the percentage of respondents who responded that they used a given app store on their smartphone. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

The survey also asked those respondents who selected multiple app stores which one they used the most. Among respondents who used multiple app stores, the Google Play Store was twice as popular

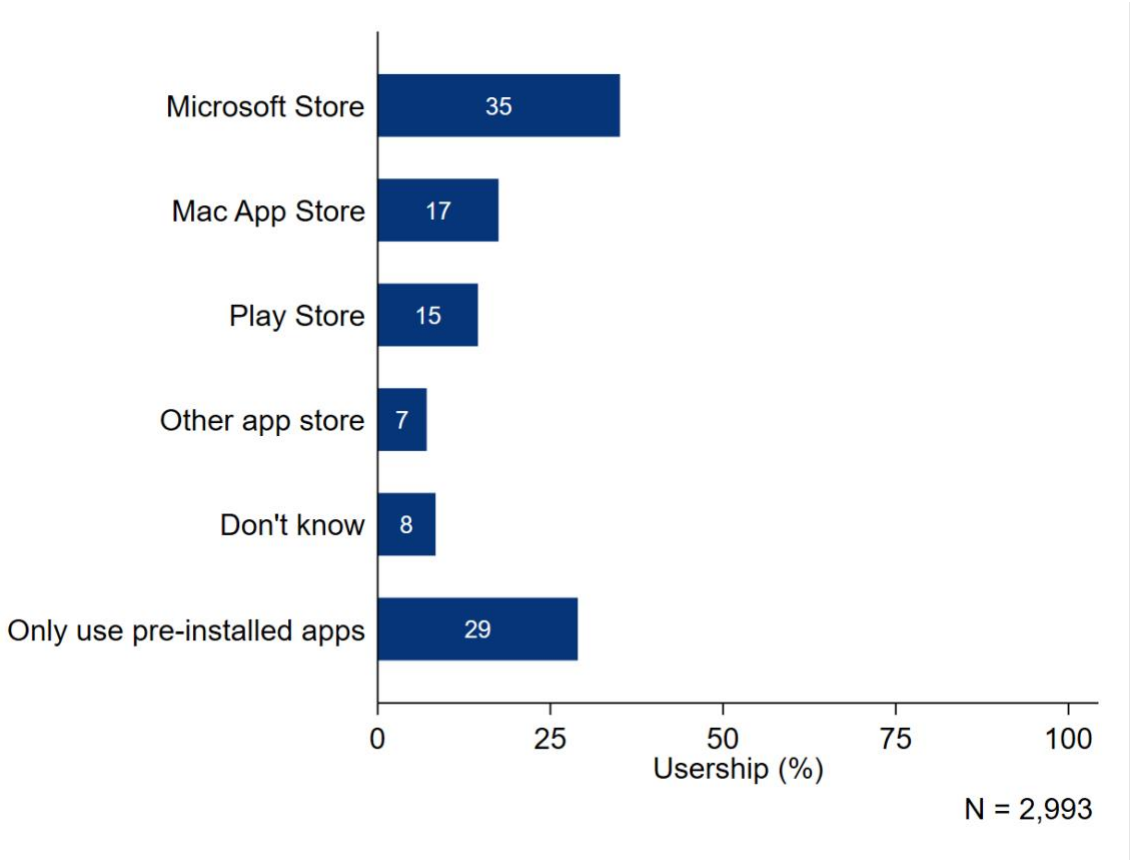
as the Apple App Store.[10] One explanation for this finding may be that users of multiple app stores were more likely to own more Android devices than Apple devices – hence relying more heavily on the Google Play Store relative to the Apple App Store. However, this cannot be directly inferred from the available data.

Laptop/desktop app store usage

Overall, the most used laptop/desktop app store was the Microsoft Store (35%) (Figure 29). However, nearly a third of respondents indicated that they only use the pre-installed apps on their laptop or desktop (29%).

Use of the Microsoft Store was relatively consistent across different demographic groups. The use of the Mac App Store by respondents located in London was around double that of any other region (30% compared to around 15% in every other region). Households with a higher income (of over £50,000) were also more likely to report using the Mac App Store than lower income groups.

Figure 29 Usage of different laptop/desktop app stores (% of respondents)



Note: The above figure shows the percentage of respondents who responded that they used a given app store on their laptop/desktop. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

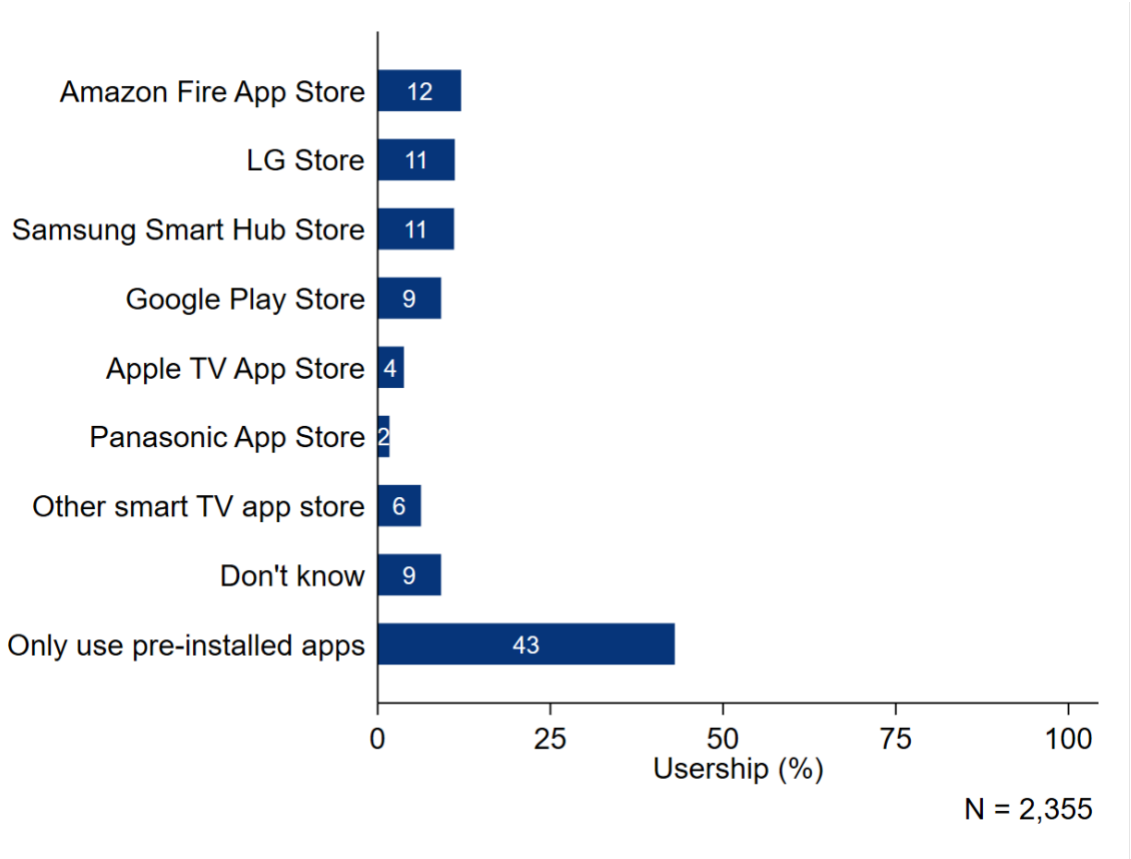
[10] Apple does not allow for third-party app stores on their devices. The survey did not ask respondents which smartphone they had, or if they had multiple smartphones. However, one hypothesis is that that those respondents who reported using both the Apple App Store and another app store (e.g. Google Play Store) have more than one smartphone. Around 10% of respondents reported to using both the Apple App Store and Google Play Store.

Smart TV app store usage

Respondents were evenly spread over the different smart TV app stores, with the most popular response being that they only use apps which were pre-installed on their smart TV when originally purchased (44%) (Figure 30).

Younger people and those with higher household income report higher usage across smart TV app stores (and are less likely to report that they only use pre-installed apps). Those with a lower level of education and those over the age of 45 were more likely than average to report that they only use the pre-installed apps on their smart TV.

Figure 30 Usage of different Smart TV app stores (% of respondents)



Note: The above figure shows the percentage of respondents who responded that they used a given app store on their smart TV. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

3.2 Consumer attitudes towards app security

The next section of the apps and app stores survey explored consumer attitudes towards app security. Specifically, the survey looked at consumer attitudes towards the accessibility of security and privacy information (Section 3.2.1), consumers' main concerns with app security (Section 3.2.2), and whether consumers felt app store operators and app developers were doing enough to protect users (Section 3.2.3).

3.2.1 Consumer attitudes towards accessibility of security and privacy information

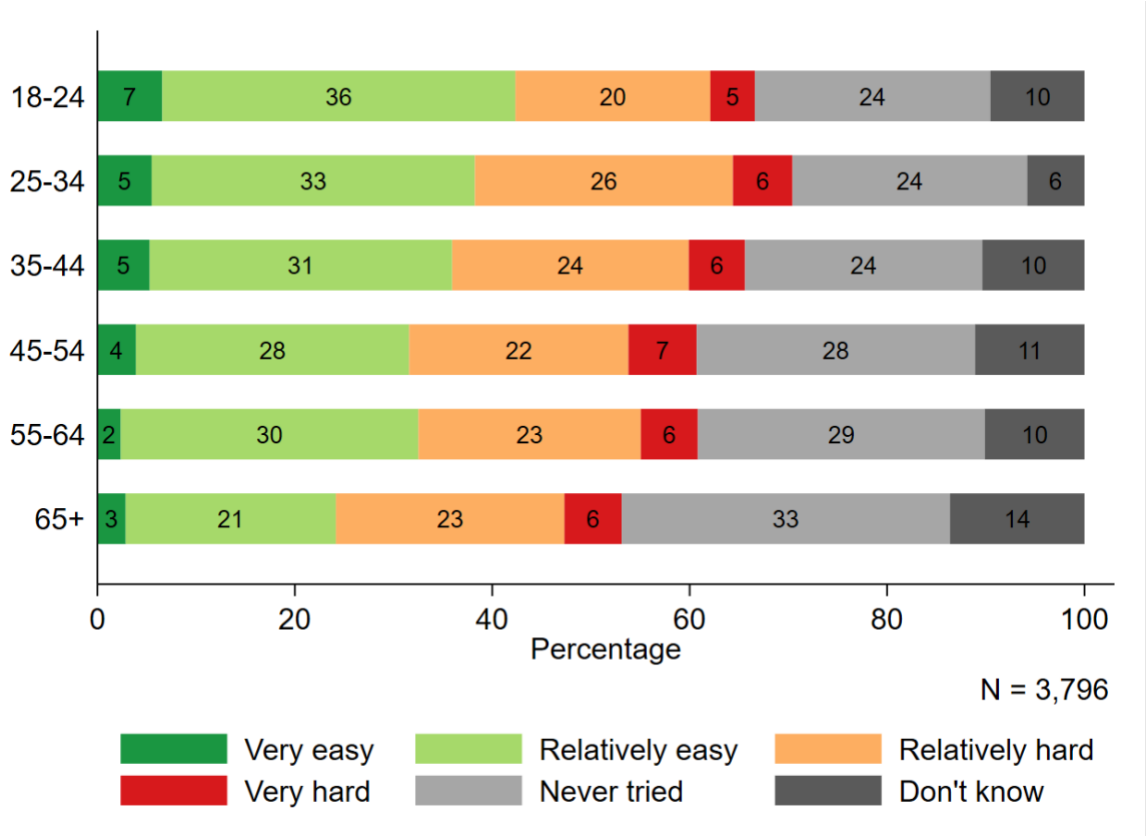
Ease of finding security and privacy information

The survey explored respondents' perceptions of how easy it is to find security and privacy information relating to an app on an app store operator or an app developer's page. In addition, it explored whether they would like to have more information displayed on, for example, how an app developer uses and shares their data.

Within the whole sample, respondents were split between whether they found it easy or hard to locate app privacy and security information. Around 33% of respondents said they found it either relatively or very easy, while 29% said they found it either relatively or very hard. Around a quarter of respondents (27%) said that they have never tried.

Across age groups, older respondents were less likely to say that they found it very easy and were more likely to say that they have never tried relative to younger respondents (Figure 31). Respondents with the highest level of education (degree-level or equivalent) were more likely to say that they found it hard to find security and privacy information compared to those with a medium level of education (A-level or GCSE equivalent).

Figure 31 Ease of finding security and privacy information on an app store or developer's page, by age group



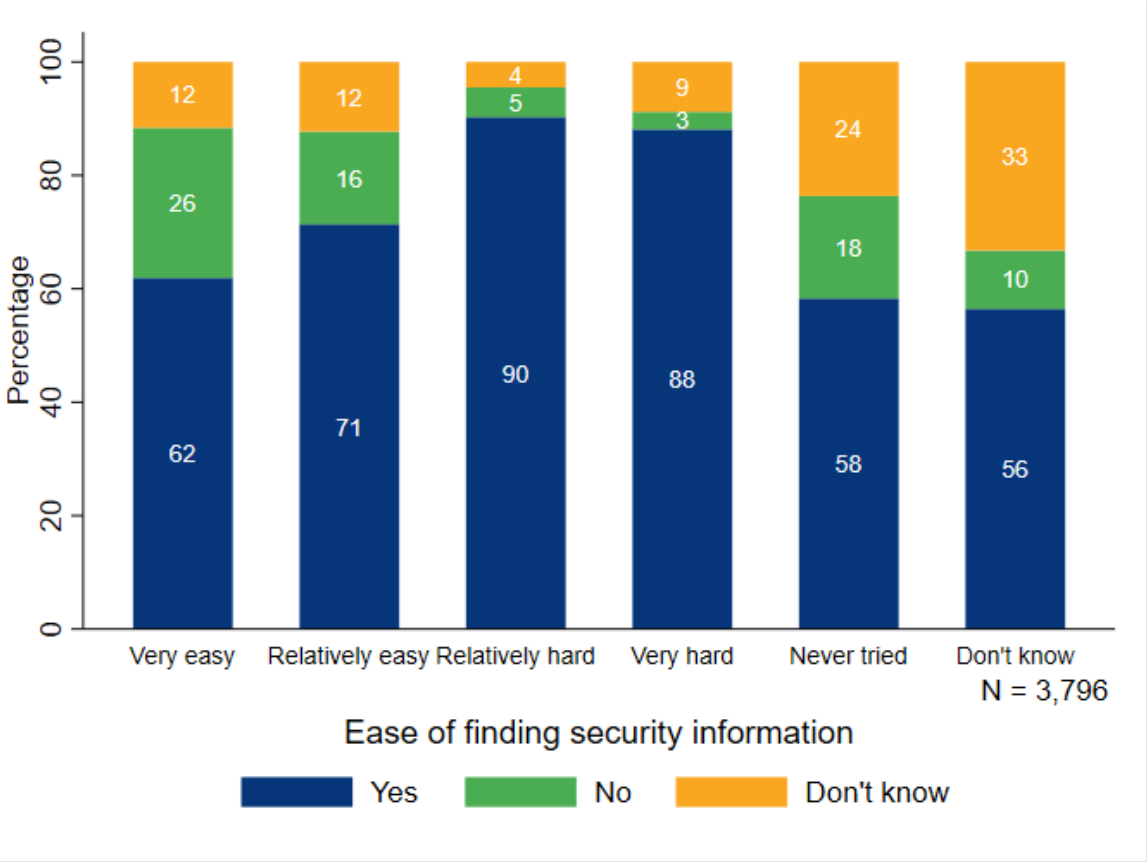
Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

Consumer preferences for more information on app security and privacy practices

The survey also asked respondents whether they would like more information regarding the security and privacy practices of an app. Respondents attitudes towards this may differ based on how easy they find it to locate such information on an app store or app developer's page, and thus know what information is currently provided. Therefore, we present the results for this question broken down by the ease at which respondents reported finding privacy and security information (Figure 32).

Out of those that found it relatively hard to locate the information, 90% would like more information on an app's privacy and security practices. By contrast, among those who find it very easy, 62% would be interested in more information.

Figure 32 Desire for more privacy and security information, by ease of locating information

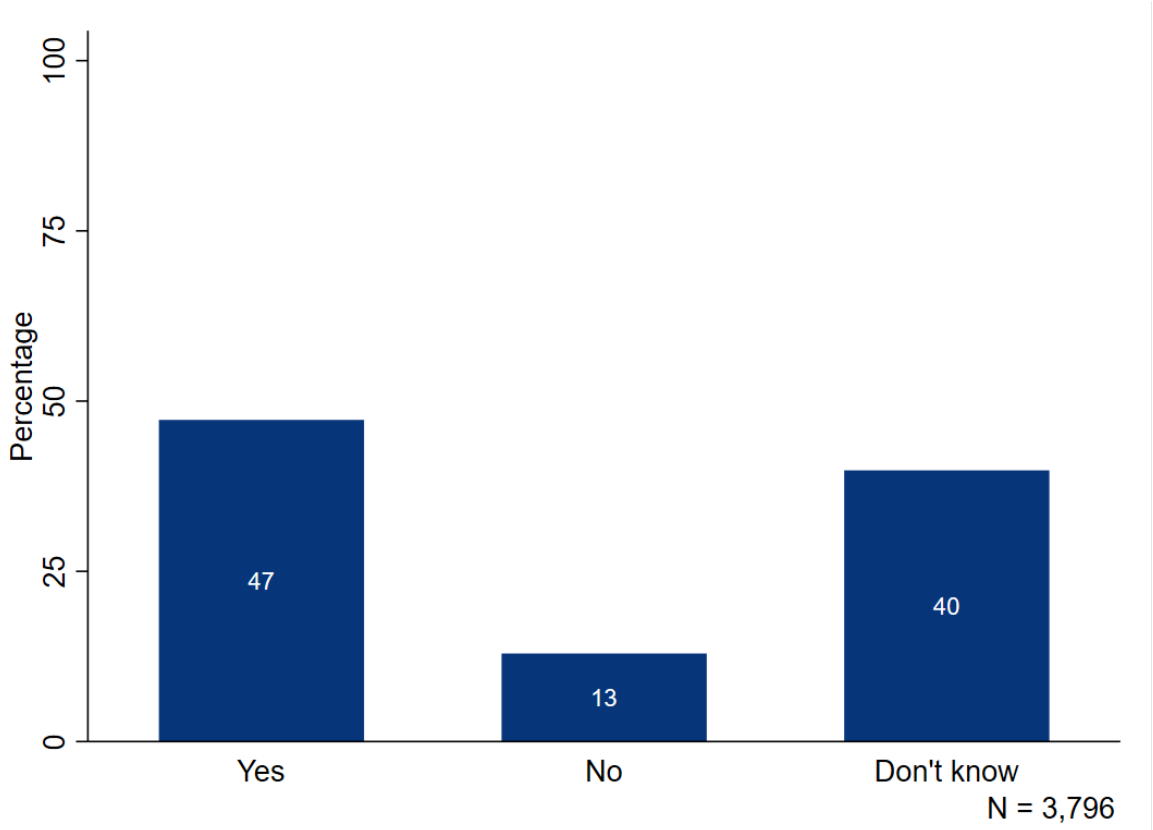


Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

Consumer perception of the security and privacy features already built into an app

Around half (47%) of survey respondents indicated that they thought that security and privacy features are already built into an app before it is ready to download on an app store (Figure 33). Around 40% of respondents indicated that they did not know, while 13% responded that they did not think security and privacy features were already built in.

Figure 33 Percentage of respondents who think security and privacy features are already built into an app before it is available to download/install on an app store



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

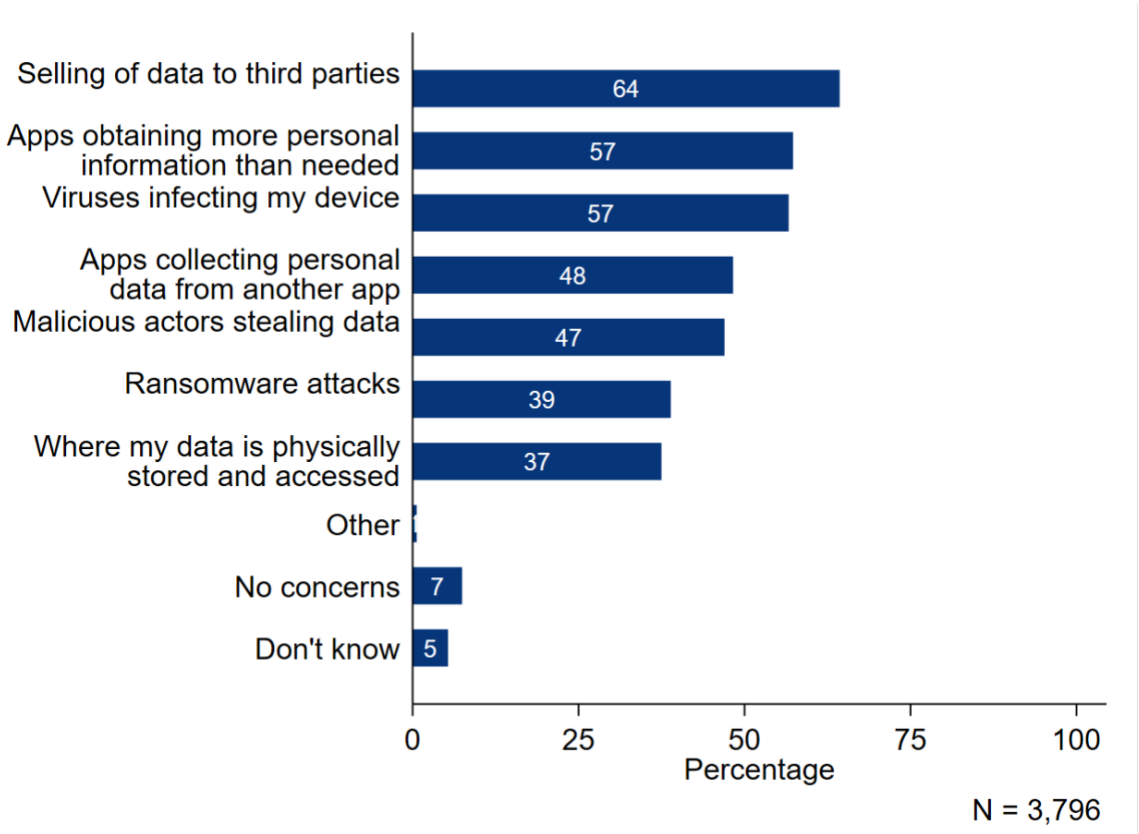
Source: London Economics/YouGov

3.2.2 Consumers' main concerns with app security

Respondents were asked to identify their main concerns with the security of apps and app stores. Overall, respondents were most concerned about their data being sold to third parties (64%), followed by apps obtaining more personal information than necessary for the functioning of the app (57%), and viruses or malware infecting their device (57%) (Figure 34). Only a small proportion of respondents reported having no concerns at all (7%).

Older age groups were more likely to report concerns around the selling of data to third parties and viruses or malware than those under 45. For example, 70% of respondents aged 55-64 reported concern over selling data to third parties compared to 52% of 18-24 year olds. Respondents with a higher level of education were more likely to report being concerned across most of the options provided, relative to respondents with a lower level of education (except for concerns over viruses or malware, which did not vary by education level). However, main concerns with app security did not vary significantly across users of different app stores.

Figure 34 Main concerns with the security of apps and app stores (% of respondents)



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

3.2.3 The extent to which consumers feel app store operators and app developers are taking appropriate steps to protect users

The next stage of the survey explored consumer attitudes towards whether app store operators and app developers are doing enough to protect users. Respondents were asked a set of identical questions pertaining firstly to app store operators and then to app developers.

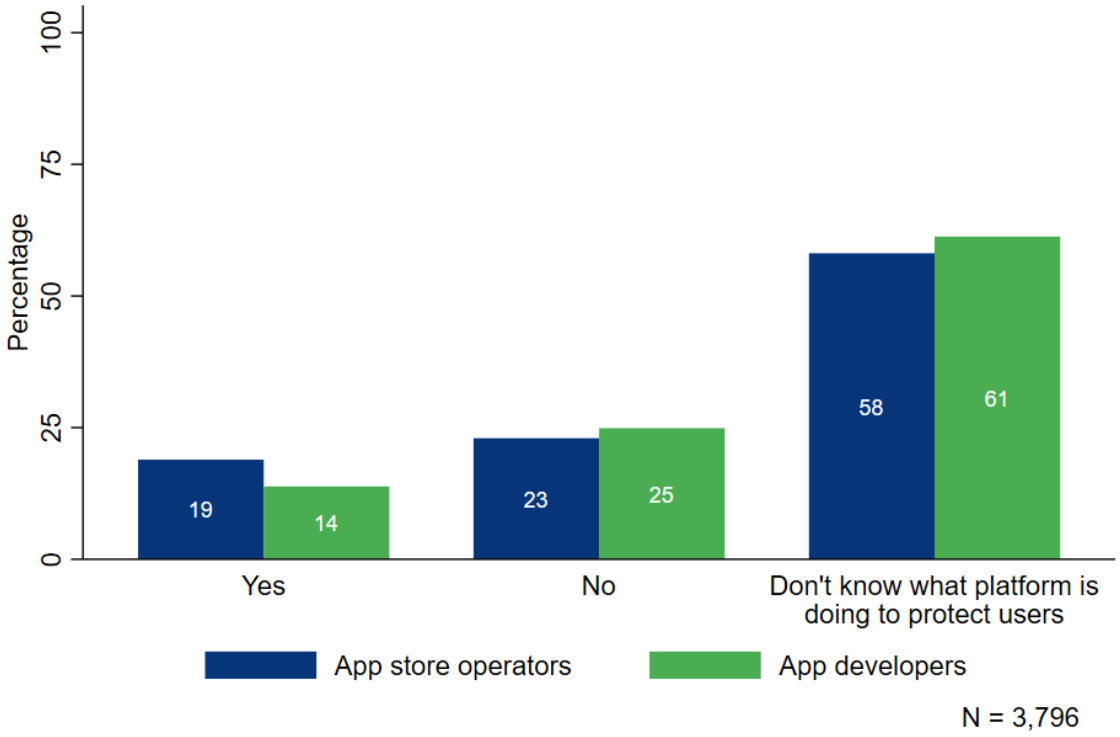
App store operators were defined as persons or organisations responsible for operating the app stores on personal devices. Examples of app store operators include Apple, Google, Microsoft, and Amazon. App developers were defined as persons or organisations which create and maintain apps available to download on the app store. App developers include for example Strava, Epic Games, and Netflix.

Respondents were first asked about their beliefs regarding whether app store operators and app developers are taking appropriate steps to protect their users. Generally, there were no significant differences between beliefs regarding how either app store operators or developers protect their users (Figure 35). For both platforms, more than half of respondents did not know what steps operators or developers put in place to protect their users (58% and 61% respectively).

Across both platforms, women were more likely to say that they did not know what steps are taken to protect them compared with men. For example, with app store operators, 66% of women said they did not know what steps are taken compared to 50% of men.

Older respondents and respondents with a lower level of education were also more likely to say that they did not know what steps were taken to protect them relative to younger age groups. This was the case for both app store operators and developers. For example, among respondents aged over 65, 67% did not know what steps app store operators were taking to protect users, compared to 52% of 18-24 year olds.

Figure 35 Percentage of respondents who believe app store operators and app developers take the appropriate steps to protect users



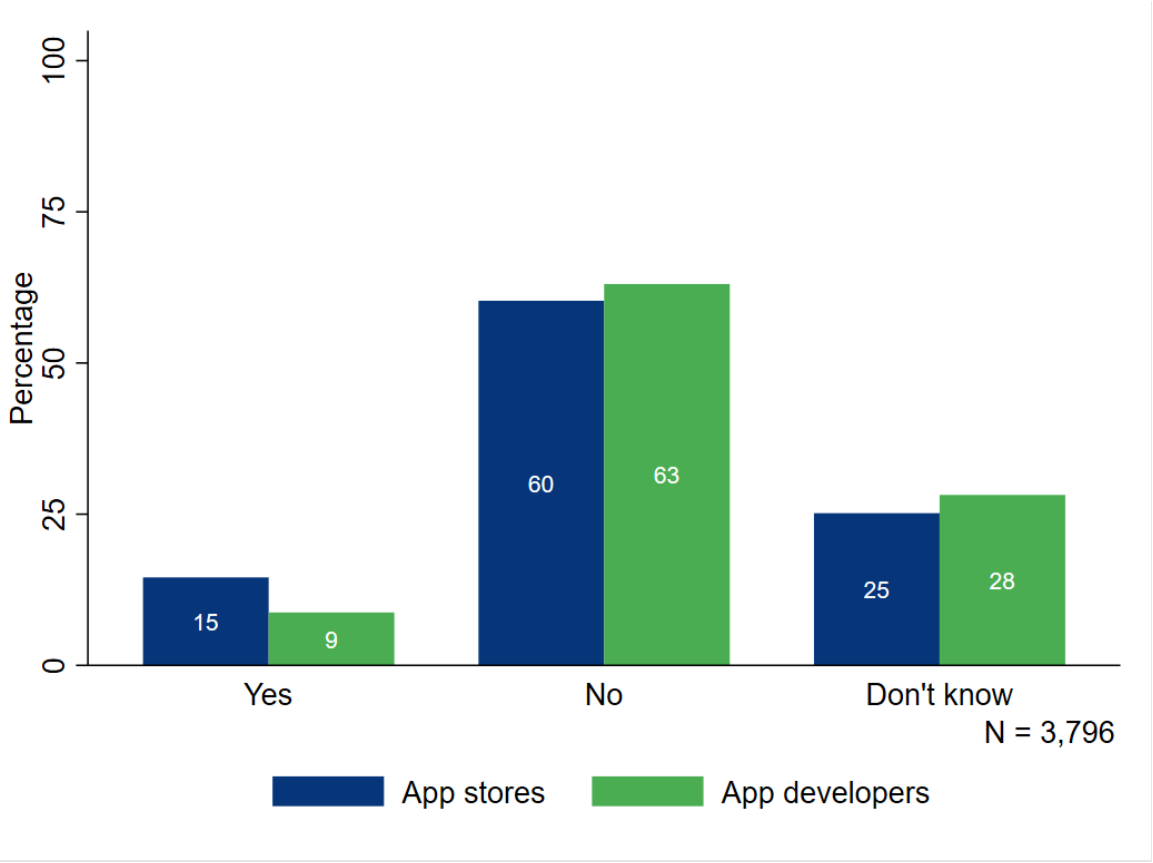
Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

Consumer experiences of privacy and security notifications from app store operators/app developers

Respondents were then asked whether they have received any privacy and security notifications from app store operators and app developers over the last 12 months. Most respondents reported that they had not received a notification from either platform over the last 12 months (Figure 36). More respondents reported receiving a notification from an app store operator than an app developer (16% vs. 9%).

The results were generally consistent across different socio-demographic groups. Respondents aged 25-34 were most likely to say they had received a privacy or security notification from an app store operator (18%) and those aged over 65 were least likely to say they had (11%).

Figure 36 Percentage of respondents who received a privacy or security notification in the last 12 months



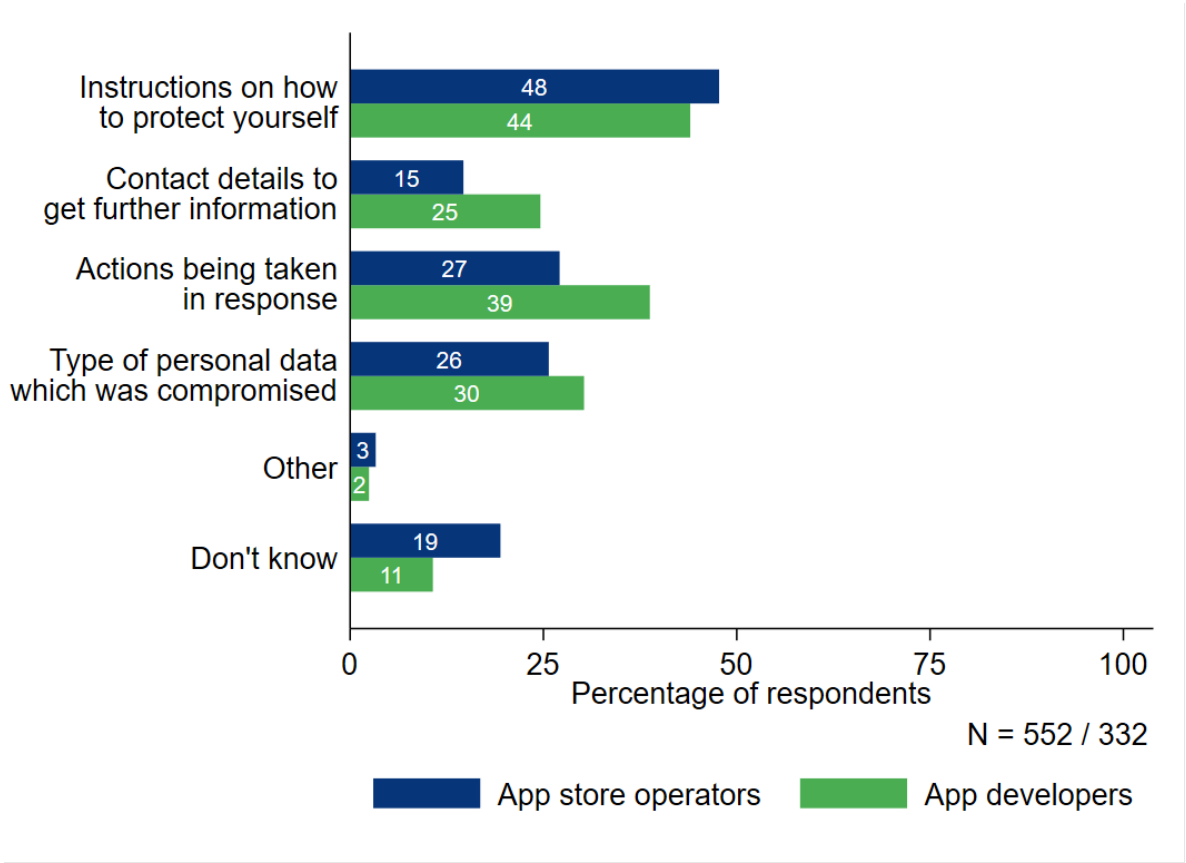
Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

Information provided to consumers in privacy or security notifications

Respondents who reported that they had received a privacy or security notification from an app store operator or app developer were then asked how the information was provided to them and what information was provided. The most popular method of receiving the information was through a notification window or alert within the app (49% for app operators and 51% for developers), followed by an email (41% for app operators and 46% for developers).

The results displaying what information was provided within the privacy or security notification are presented below in Figure 37. The most common type of information received by respondents from app store operators and app developers was instructions on how to protect themselves (48% and 44% respectively).

Figure 37 Type of information provided by security notification



Note: The chart uses the weighted sample base. The sample sizes N are shown in the bottom righthand corner. The sample size of 552 refers to the sample of those who said they had received a privacy notification from an app store and the sample size of 332 refers to the sample of those who said they had received a notification from an app developer. Therefore, the bars represent the number of respondents as a proportion of the respective sample sizes.
Source: London Economics/YouGov

3.3 Consumer behaviours towards app security

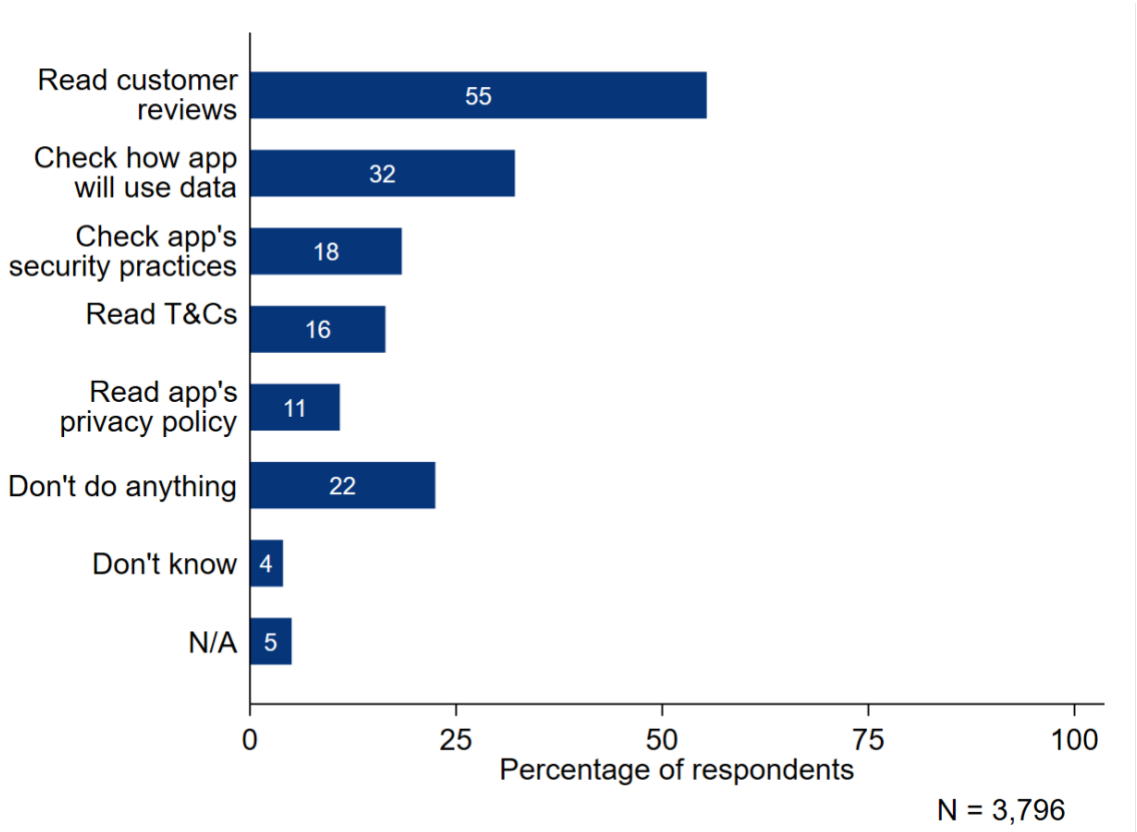
The following section explores consumer attitudes towards the security of apps and app stores. Section 3.3.1 examines consumer behaviours when downloading apps – specifically actions taken before and after downloading an app. Section 3.3.2 explores the extent to which consumers are willing to pay a premium for enhanced security across different types of app.

3.3.1 Consumer behaviours when downloading apps

Actions taken before downloading apps

Survey respondents were asked to specify what actions they took before and after downloading apps onto their devices. The percentage of respondents taking different actions **prior** to downloading an app is shown in Figure 38. The most common action was reading customer reviews (55%), followed by checking how the app will use consumer data (32%). Around one quarter (22%) of respondents said they do not do anything prior to downloading an app.

Figure 38 Percentage of respondents who reported taking different actions before downloading app



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

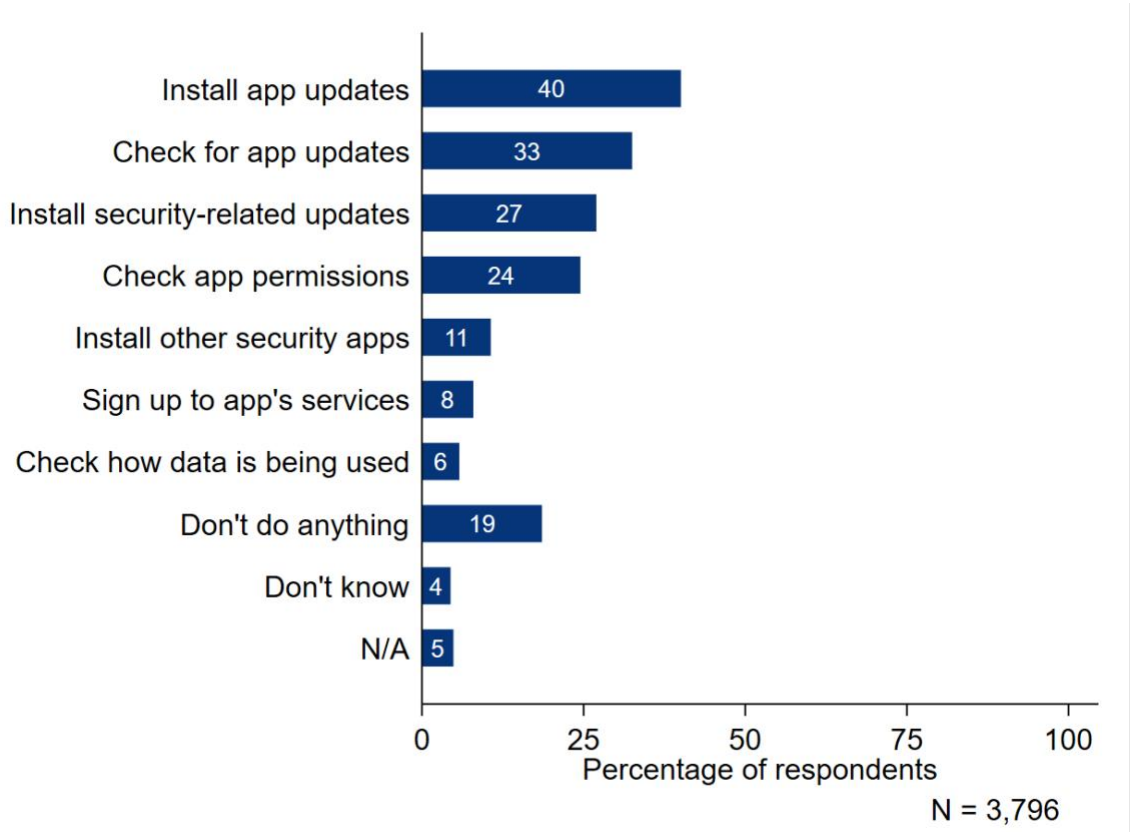
Actions taken after downloading apps

The proportion of survey respondents taking different actions **after** downloading an app is displayed in Figure 39. Among respondents who took some action, the most common actions were to install app updates (40%), check for app updates (33%), and install security-related updates (27%).

Older respondents and respondents with a lower household income were more likely to report not doing anything after downloading an app. Specifically, 21% of respondents over 65 reported that they did not do anything, compared to 15% of 18-24 year olds. Around 20% of respondents with an annual household income of below £25,000 reported not doing anything, compared to 13% of those with a household income above £100,000.

Combining the findings from Figure 38 and Figure 39, around 8% of respondents indicated that they did not do anything both before, and after, downloading an app.

Figure 39 Percentage of respondents who reported taking different actions after downloading app



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

3.3.2 Consumer willingness to pay for enhanced app security

To explore whether consumers are willing to pay more for enhanced app security, survey respondents were asked to state the premium they would be willing to pay for improvements in cyber security when purchasing apps. Specifically, respondents were asked to state the percentage price premium (for example a 10% premium) they would be willing to pay for an app in return for either a 50% or 90% reduction in the number of security incidents or breaches relating to that app each year.

Respondents were randomly allocated to be shown a 50% reduction or a 90% reduction in the number of incidents. Respondents were also asked to report their willingness to pay separately for four different categories of app – gaming or entertainment, finance, health and fitness, and productivity and education.

As for the IoT willingness to pay exercise, it should be noted that the willingness to pay questions in this section were not embedded within a full stated preference analysis, as this would have required a separate standalone survey. Therefore, the results in this section should be interpreted with caution.

Across all categories of apps, more than half of respondents were not willing to pay any more for enhanced app security. For example, 70% of respondents said they would not be willing to pay anything more for a 50% improvement in the security of a gaming or entertainment app.

Willingness to pay for enhanced app security, among people who have experienced a cyber security issue with apps or app stores

Respondents that had previously experienced a security issue had a higher willingness to pay for increased security when compared with respondents who had not experienced a security issue. For example, 43% of respondents who had experienced a security issue indicated that they would be willing to pay a premium for enhanced security, compared to 30% in the full sample. These results suggest that consumers who directly experience a security issue with their apps or app stores are more willing to pay a premium for improved app security.

Below, Table 3 shows the mean willingness to pay for enhanced app security, by app type and percentage improvement in security. Overall, respondents were willing to pay more for a 90% improvement in app security against a 50% improvement.

This finding suggests that consumers are responsive to changes in the degree of security enhancement when purchasing apps. However, the difference in mean willingness to pay between a 50% improvement in security and a 90% improvement in security was relatively small (between 1-3 percentage points depending on the type of app).

Respondents had a higher willingness to pay for security improvements relating to finance apps. The mean percentage premium for a 50% improvement in security was 21% for finance apps, compared to 10-12% for the other categories of app. This finding may reflect the fact that security is a more salient concern for survey respondents in relation to financial matters.

Taking the results for a 50% improvement in device security, there is a statistically significant difference between the mean willingness-to-pay for finance apps compared to all other app types[11].

Table 3 Mean willingness to pay (percentage premium) for enhanced security, by app type

App type	50% improvement in security	90% improvement in security
Gaming or entertainment	10%	12%
Finance	21%	24%
Health and fitness	11%	12%
Productivity and education	12%	15%

Source: London Economics/YouGov

There was little difference in the mean percentage willingness to pay for different app types across income groups, although respondents with a higher household income had a higher mean willingness to pay. This result could reflect the fact that apps are generally relatively cheap, so income may not be particularly constraining when thinking about the premium consumers would be willing to pay for improved security.

Particular caution is needed when interpreting the percentage premium for apps, as they are typically free to download. However, we assume that a positive percentage premium reflects a willingness to pay a positive amount to avoid security issues. Additionally, the relative premiums across different categories (e.g., gaming or entertainment vs. finance) suggest that respondents are willing to pay more for the security of finance apps compared to gaming or entertainment apps.

[11] The null hypothesis is rejected at the 95% significance level.

3.4 Consumer experiences and impacts of cyber security issues for apps and app stores

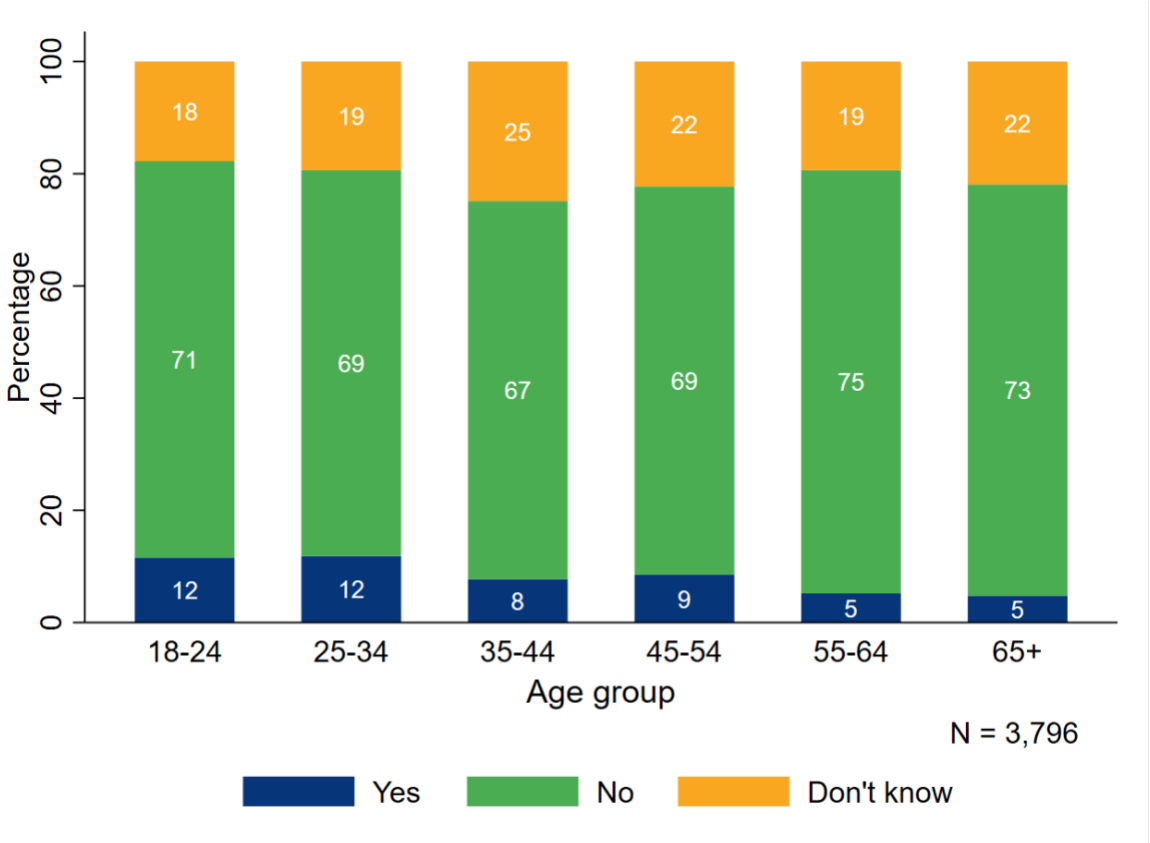
The next section of the report looks at consumer experiences of cyber security issues relating to apps and app stores. First, Section 3.4.1 provides descriptive information on whether consumers had experienced a cyber security issue, and – if yes – the number of issues experienced. Next, Section 3.4.2 examines the impacts reported by people who experienced a cyber security incident. Finally, Section 3.4.3 details changes in consumer behaviour following a cyber security incident.

3.4.1 Consumer experiences of cyber security issues

Respondents were first asked if they had experienced a cyber security issue relating to apps or app stores. Across the whole sample, most respondents either reported that they had not experienced an issue with apps or app stores (71%) or did not know whether they had (21%), with only 8% of respondents reporting that they had experienced a cyber security issue.

The percentage of respondents who reported experiencing a security issue varied with age. As displayed in Figure 40, younger age groups (18-24 and 25-34 year olds) were around twice as likely to report experiencing a security issue than older age groups (55-64 and over 65s). The percentage of people who reported that they had experienced a security issue was 12% for the youngest age groups, compared to 5% for the oldest.

Figure 40 Percentage of respondents who reported experiencing a cyber security issue with apps or app stores, by age group



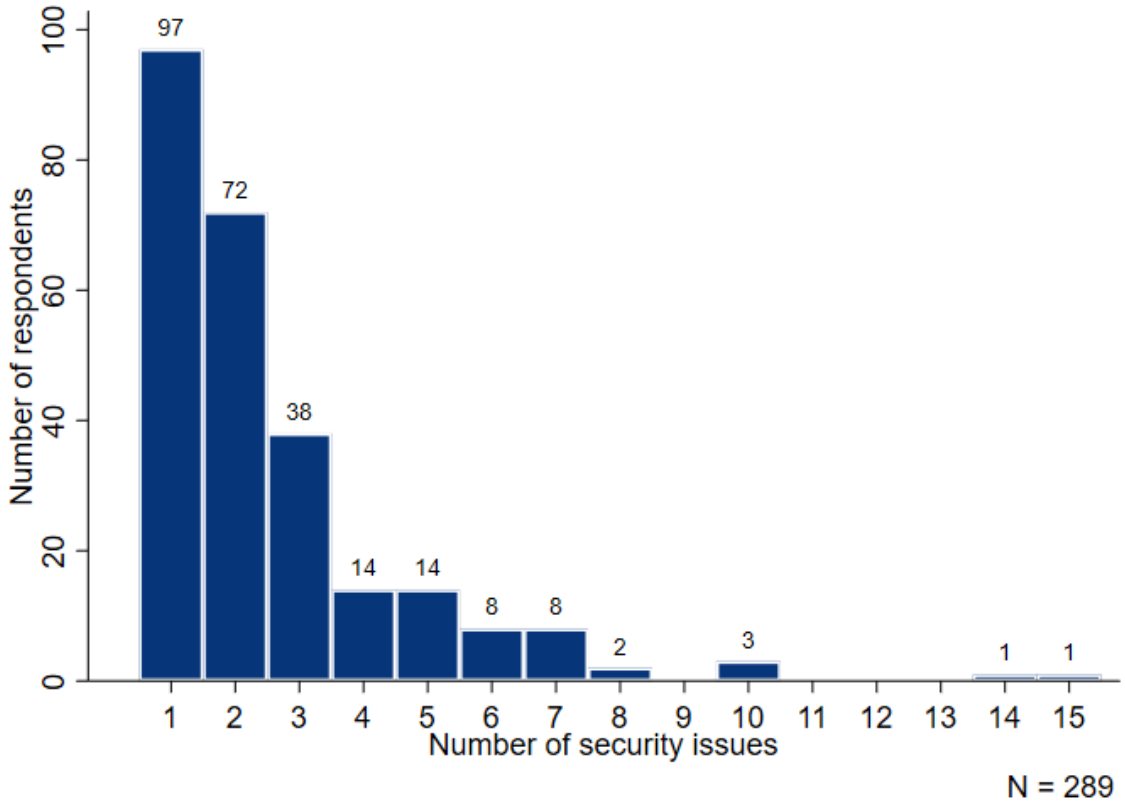
Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

The number of cyber security incidents experienced by consumers with apps or app stores

Respondents who reported experiencing a security issue with their apps or app stores were asked to estimate how many security issues they had experienced. Among people who had experienced an incident, most had reported that they had experienced fewer than five incidents (Figure 41). Out of 289 respondents who had reported having experienced an issue, 235 (81%), reported five or fewer incidents.

Figure 41 Histogram of number of security incidents relating to apps or app stores



Note: Each bar corresponds to a different number of security issues – for example the first bar counts the number of respondents experiencing one issue.

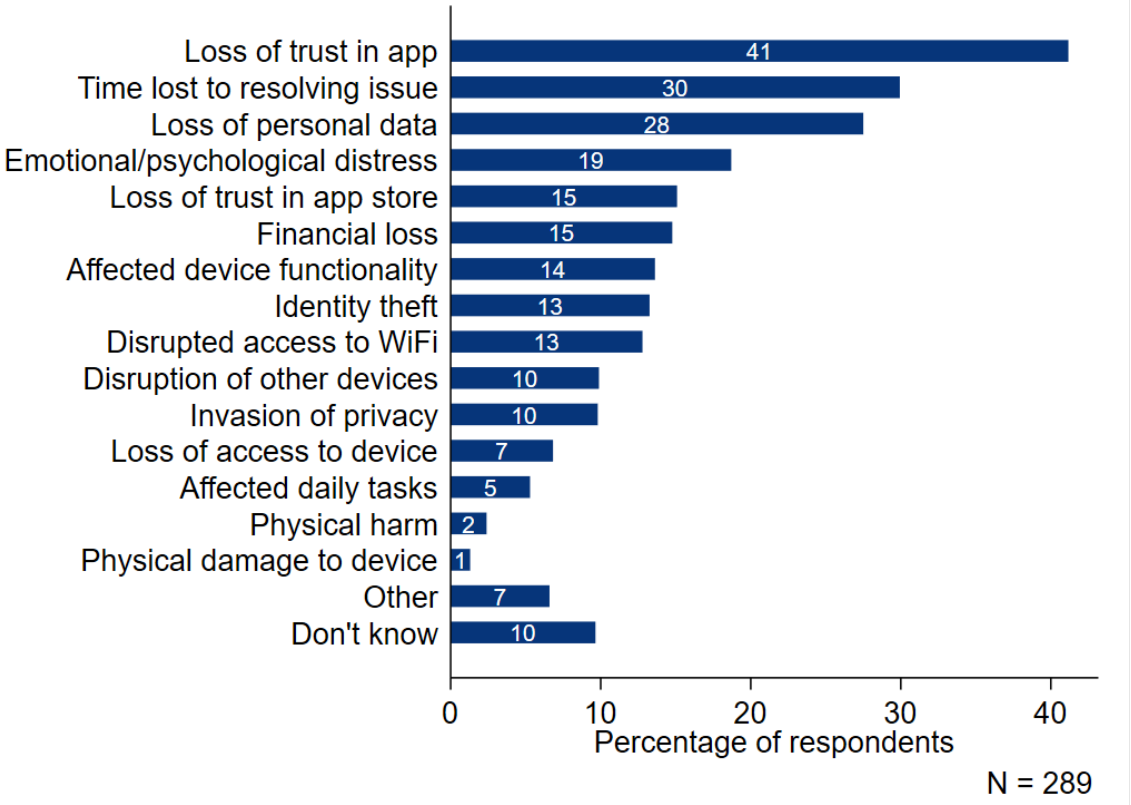
Source: London Economics/YouGov

3.4.2 Consumer impacts of cyber security issues

Reported harms from a security incident relating to apps or app stores

Experiencing a cyber security issue can result in a variety of impacts, including financial or emotional harm. To explore the impacts of cyber security issues relating to apps and app stores, survey respondents who reported experiencing an incident were asked to identify which impacts they had suffered (Figure 42). The most common impact was a loss of trust in the affected app (41%), followed by time lost resolving the issue (30%) and emotional or psychological distress (19%).

Figure 42 Percentage of respondents reporting different types of harm resulting from security incident relating to apps or app stores



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

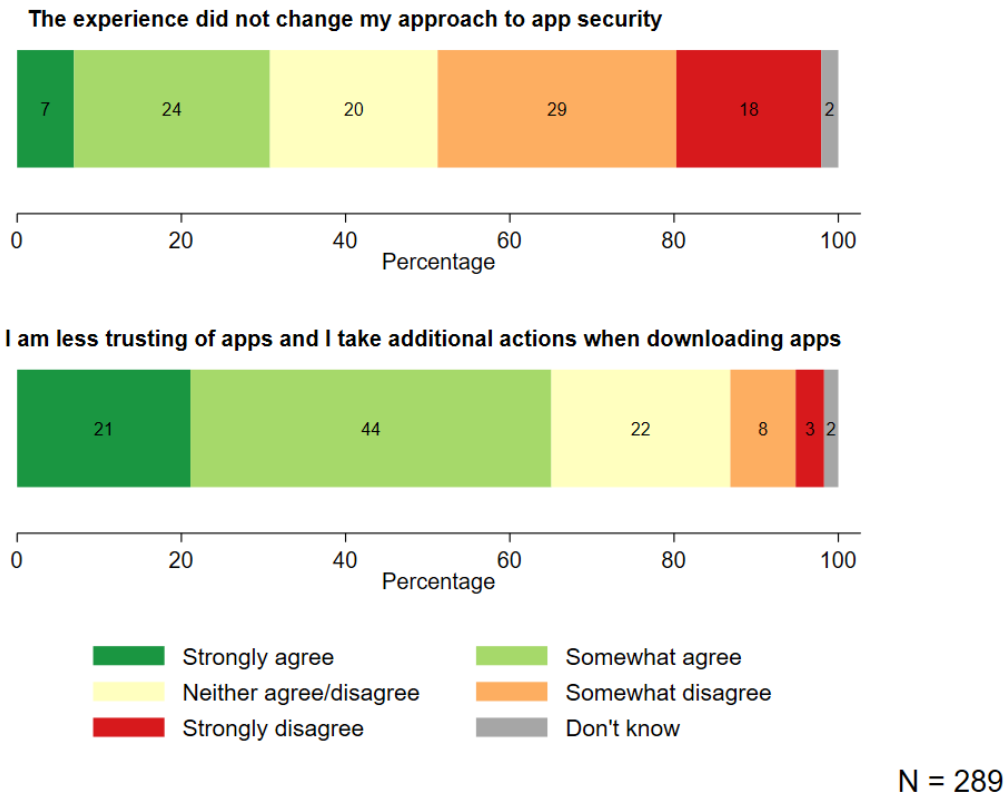
Consumer attitudes to apps and app securities following a security incident

To develop a deeper understanding of the impacts of cyber security incidents to do with apps and app stores, survey respondents who reported experiencing security incidents were asked to indicate the extent to which they agreed or disagreed with several statements. Specifically, respondents were asked the extent to which they agreed or disagreed with the following statements:

- "The experience did not change my approach to cyber security."
- "I am less trusting of apps, and I take additional actions when downloading apps."

Around half (47%) of people who had suffered a security issue indicated that their approach to app security had changed due to the issue (Figure 43). Similarly, 65% of respondents agreed or strongly agreed that they were less trusting of apps and took additional actions when downloading apps.

Figure 43 Responses to statements regarding impacts of cyber security issue with apps or app stores, among people who experienced an issue



Note: The chart uses the weighted sample base.

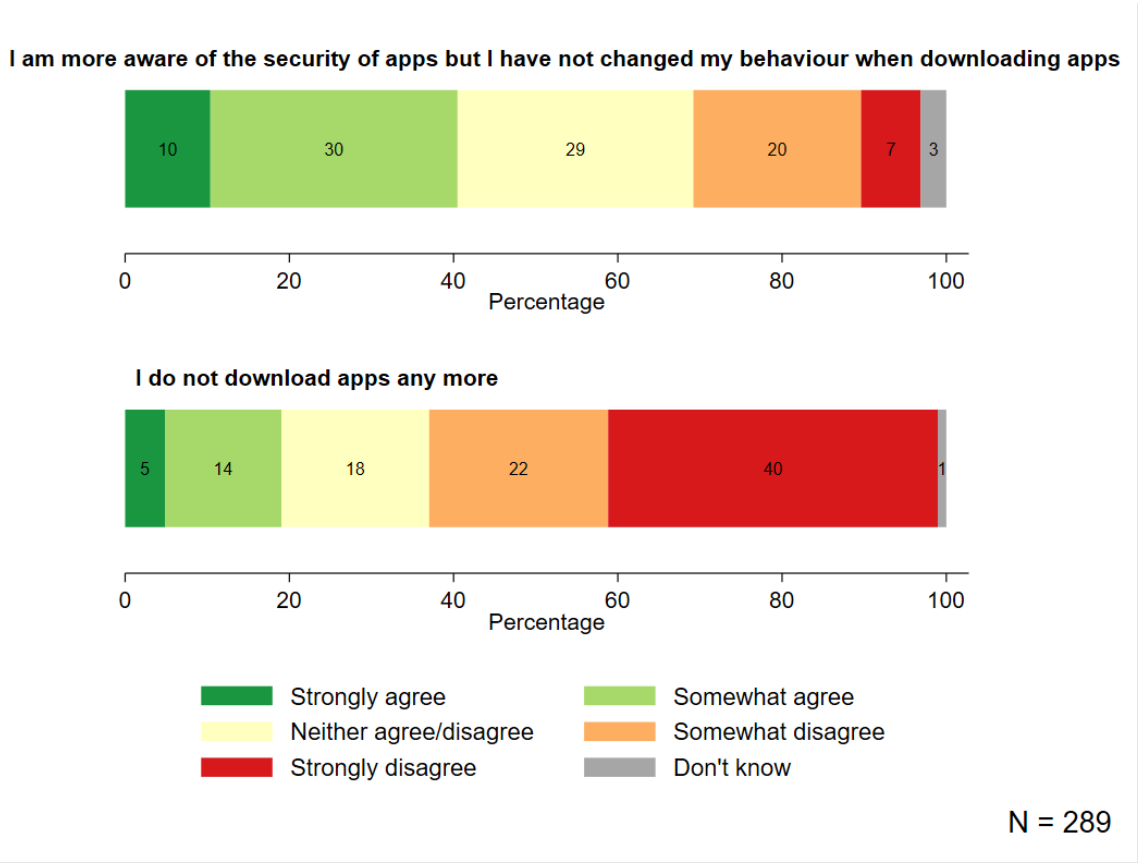
Source: London Economics/YouGov

3.4.3 Consumer behaviours following cyber security issues

Awareness of app security and avoidance of downloading apps

In addition to the impact of experiencing a cyber security issue, the survey explored how individual behaviours changed following this experience. Figure 44 shows that 40% of respondents said that they are more aware of security of apps but have not changed their behaviour when downloading apps, compared to 27% who disagreed with the statement. Just under 1 in 5 (19%) of respondents agreed that they did not download apps anymore.

Figure 44 Responses to statements regarding behaviours following a cyber security issue with apps or app stores, among people who experienced an issue



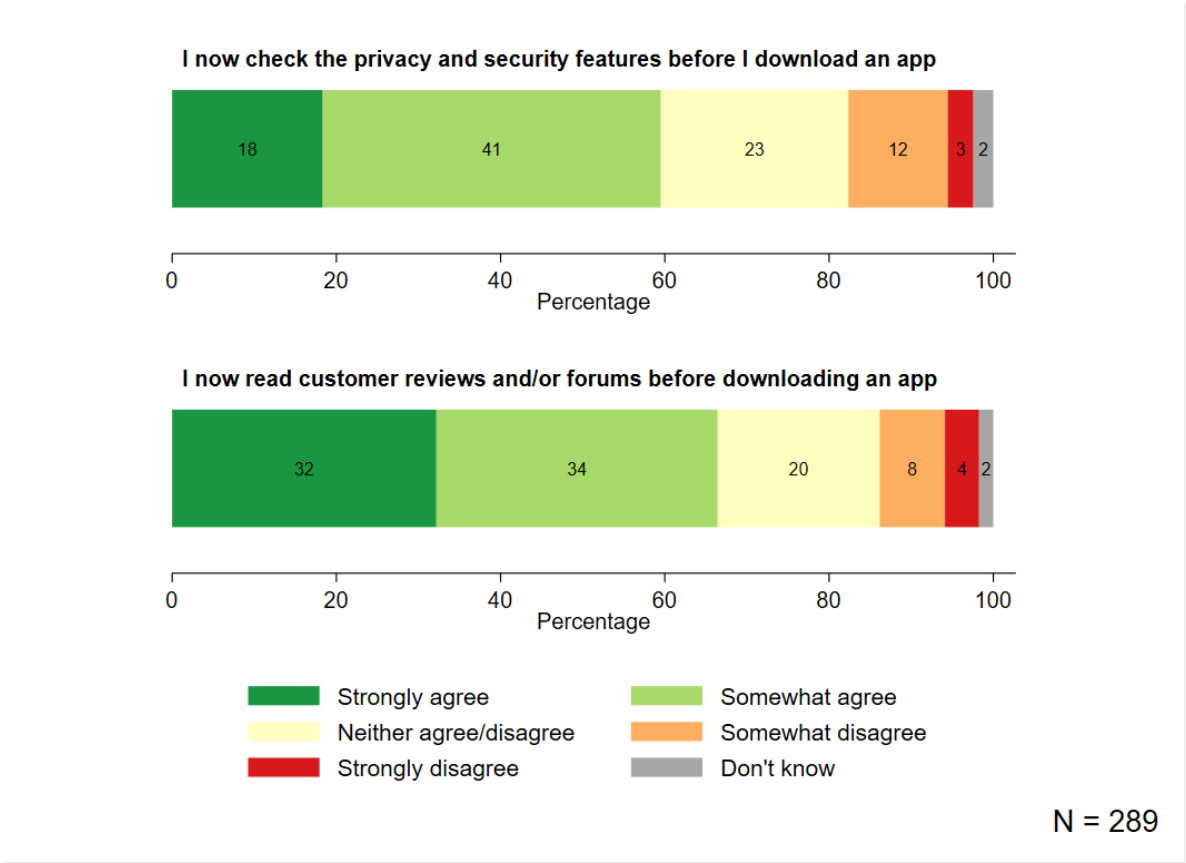
Note: The chart uses the weighted sample base.

Source: London Economics/YouGov

Additional actions undertaken prior to downloading apps

As shown in Figure 45, over half of respondents either agreed or strongly agreed that they checked the privacy and security features before downloading apps (59%) and that they read customer reviews before downloading apps (66%). Together with the results in Figure 43, these findings imply that most people who experience a cyber security issue change their attitude towards apps and app stores and take additional actions when downloading apps.

Figure 45 Responses to statements regarding behaviours following a cyber security issue with apps or app stores, among people who experienced an issue



Note: The chart uses the weighted sample base.

Source: London Economics/YouGov

Respondents who indicated that they now took additional actions when downloading apps (having already experienced a cyber security issue) were asked to explain the actions they took in an open text question. The key responses to emerge from this question were:

- doing more research online about the app and reading customer reviews to be more selective (e.g. not downloading apps with few or zero reviews);
- preferring to use well-known or trusted platforms (respondents referred to examples such as the Apple App Store);
- minimising the amount of data shared with app store operators and developers, sometimes entering random information to avoid giving away personal data;
- using stronger passwords and changing them more regularly;
- stopping to consider whether the app is necessary before downloading it; and
- using additional layers of internet protection such as VPNs, firewalls, and ad-blockers.

3.5 Consumer attitudes to the Code of Practice for app stores and app developers

In October 2023, the UK Government published an updated version of the voluntary Code of Practice setting out the baseline security and privacy requirements for app store operators and app developers. The main objective of the Code of Practice is to ensure that app store operators and

app developers protect app users. Within the Code of Practice is a requirement to provide consumers with more information about an app's security and privacy practices.[12]

To test consumer understanding of the updated Code of Practice and its implications for security and transparency, respondents were presented with information about the Code, including some of its key requirements for app store operators and developers. The following text was shown to respondents:

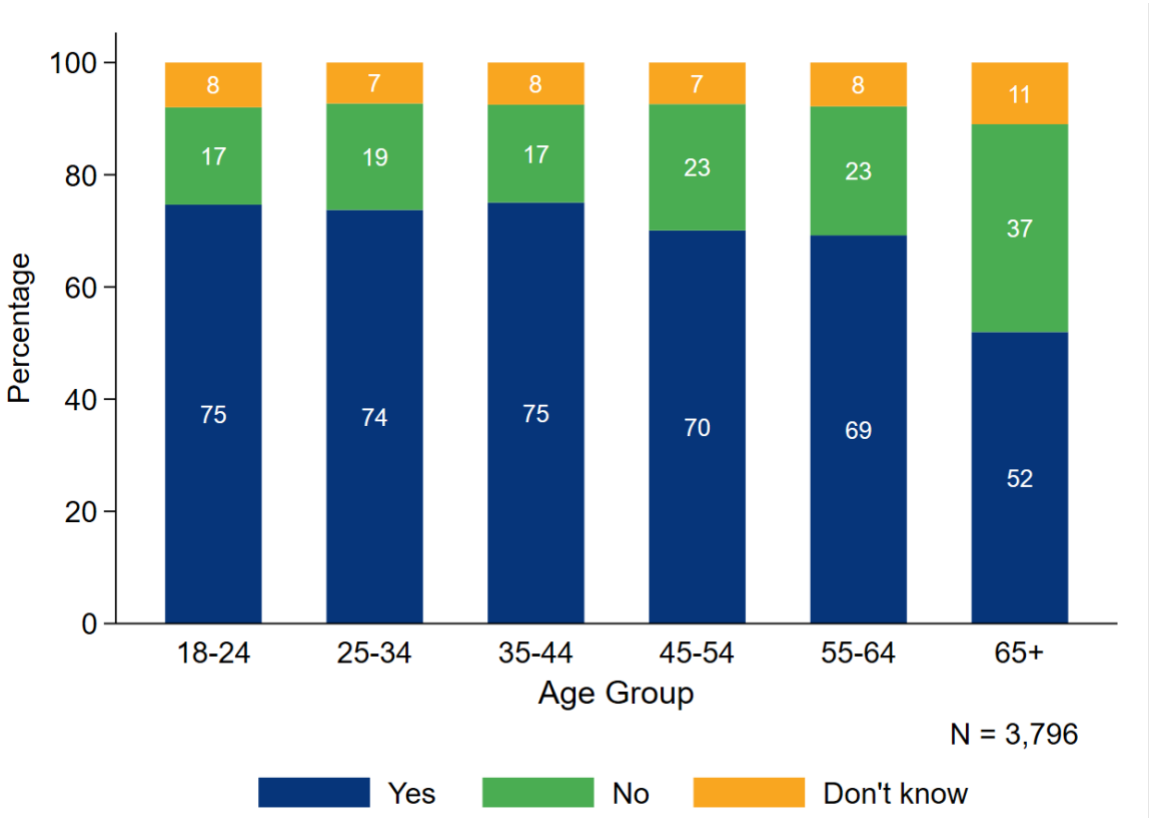
"The Government has published a Code of Practice that sets baseline security and privacy requirements for developers and app store operators. Within the Code of Practice is a requirement to provide consumers with more information about an app's security and privacy practices. This includes:

- *The jurisdictions where a user's data is stored and processed for each app.*
- *The stakeholders that are given access to a user's data.*
- *The categories of stakeholders that are displayed to a user should include third party companies, the app's organisation, specific governments or [is] not shared with anyone.*
- *The purpose of accessing or using a user's data.*
- *When the app was last updated and any other relevant security information, such as permissions."*

Respondents were asked whether they understood the information. Comprehension of the updated Code of Practice was roughly similar across age groups apart from the over 65 age group, who were less likely to respond that they understood the information (Figure 46). Only 52% of people in this age group reported that they understood the information in the Code of Practice. This was 17 percentage points lower than the second lowest percentage of 69% (for 55-64 year olds).

[12] Department for Science, Innovation, and Technology (2022) Code of Practice for app store operators and app developers

Figure 46 Percentage of respondents who report that they understand the information in the new Code of Practice, by age group



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

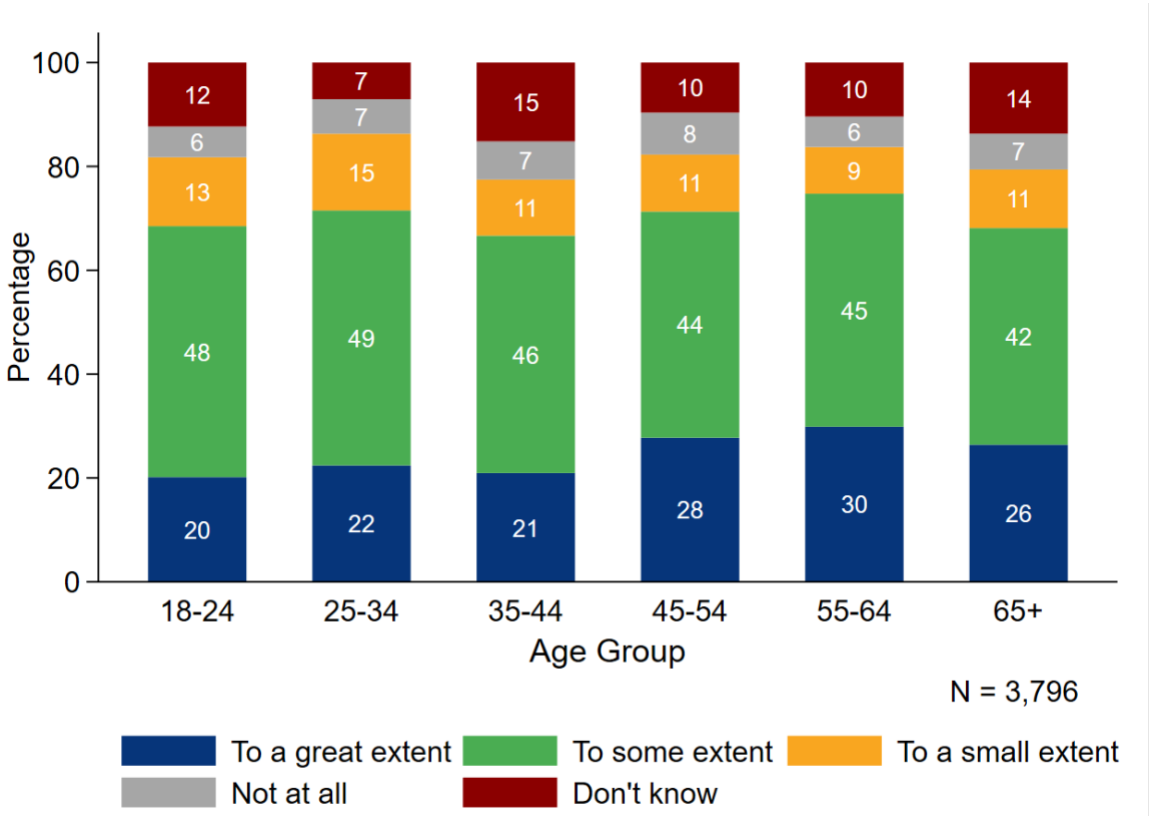
Extent to which consumers would prioritise an app store if it had implemented the voluntary Code of Practice

Survey respondents were asked if they would prioritise using an app store if it had publicly stated that it had implemented the security and privacy requirements set out in the updated Code of Practice. The results suggest that across age groups, respondents would prefer app stores which implement the guidelines in the Code of Practice (Figure 47). Across age groups, 75-85% of respondents indicated that they would prioritise such an app store at least to a small extent.

There was relatively little variation across age, even though older respondents were less likely to state that they understood the information contained within the Code of Practice. This finding may imply that consumers interpret the Code of Practice as ensuring that they are protected when using an app store, even if they do not understand the specific information covered by the legislation.

Respondents with a household income of less than £25,000 per year were less likely than any other income group to say they would prioritise an app store if it had implemented the Code of Practice (79% of respondents in this group said they would prioritise an app store, at least to a small extent, if it had implemented the Code of Practice, compared to 85-87% among other income groups).

Figure 47 Percentage of respondents who report that they would prioritise an app store if it had implemented the new Code of Practice, by age group



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

4 Connected places

The survey explored respondents' knowledge and perception of connected places (or 'smart cities'). A connected place was defined as:

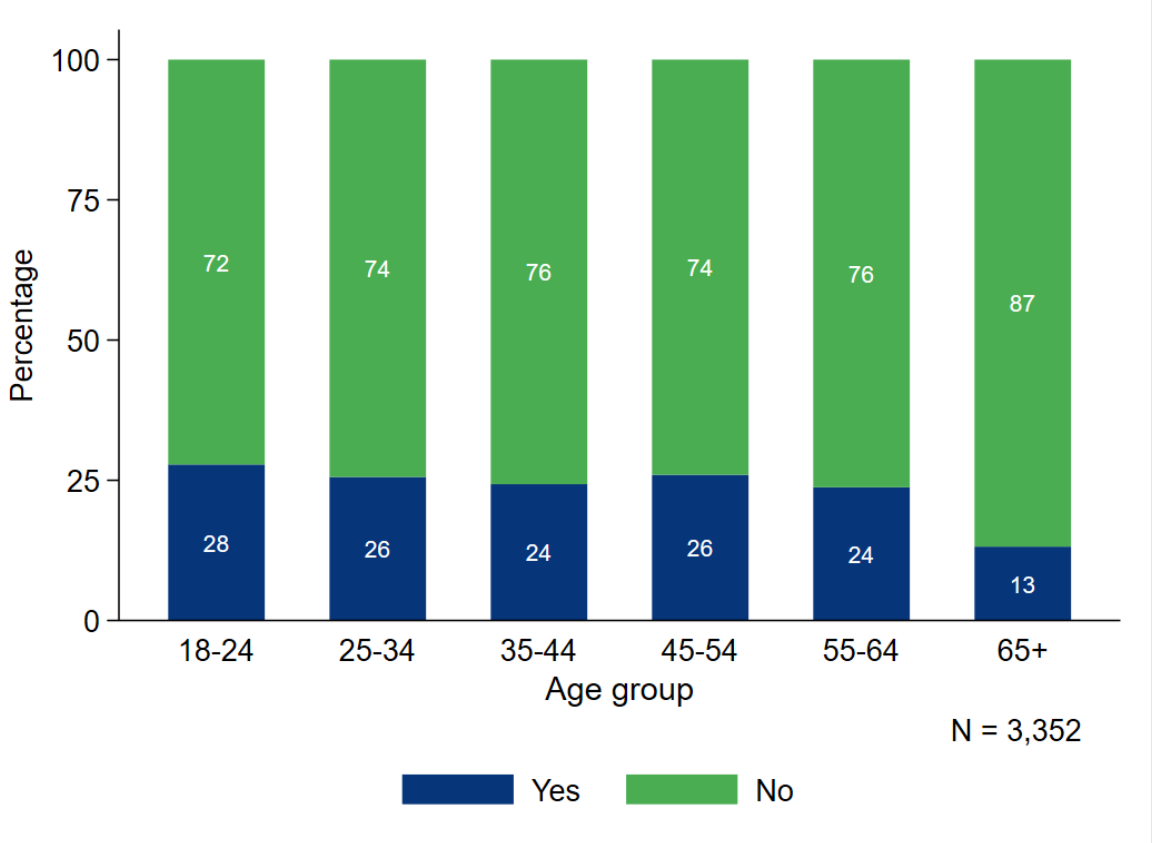
"a community that integrates IT technology and IoT devices to collect and analyse data to deliver new services to the built environment and enhance the quality of living for citizens." [National Cyber Security Centre]

Respondents were asked whether they were aware of the concept of connected places and whether they had seen any examples of connected places technology in their local area (Section 4.1), and their perceptions of various types of connected places technology (Section 4.2).

4.1 Consumer awareness of connected places or smart cities

A larger proportion of people stated that they did not know what a connected place was compared to those that did. Across the full sample, 77% of respondents indicated that they did not know what a connected place was. These findings were consistent across age groups (Figure 48). The percentage of people indicating that they did not know what a connected place was ranged from 72% for 18-24 year olds to 87% for over 65 year olds.

Figure 48 Percentage of respondents who reported knowing what a connected place or smart city is, by age



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

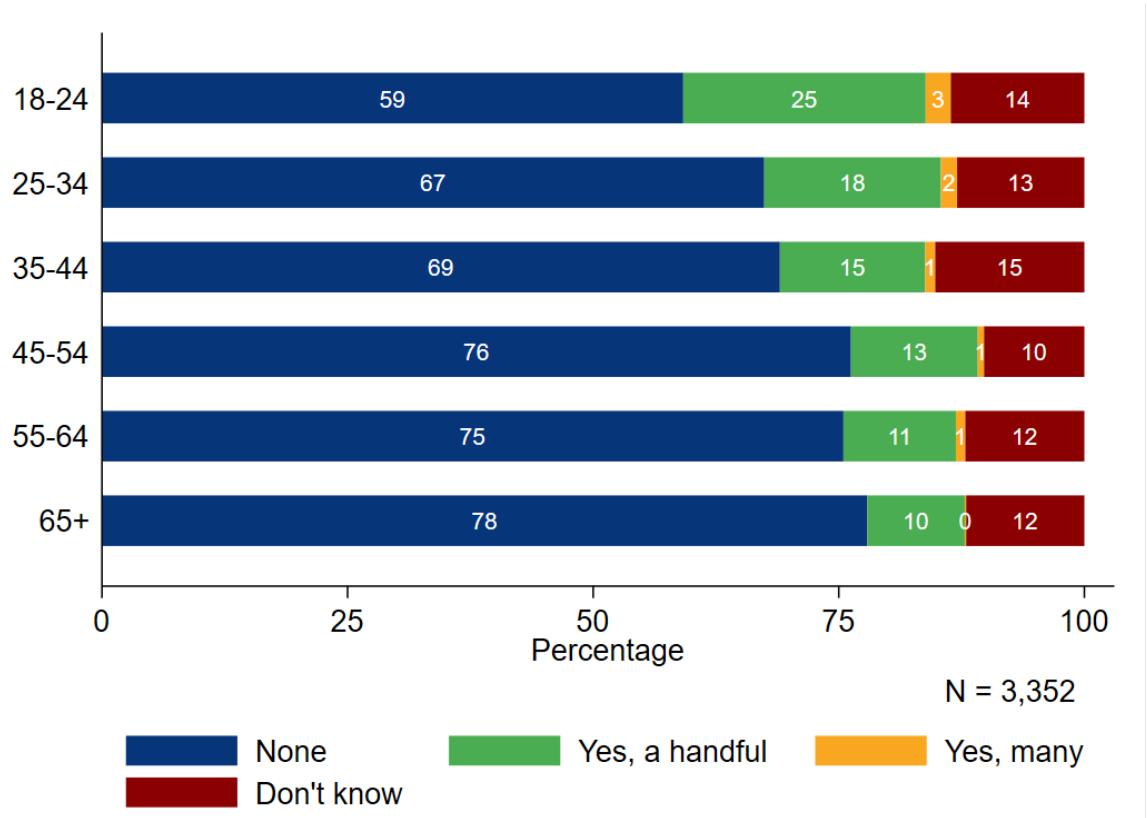
Higher income households were more likely to report awareness of what a connected place was than lower income households. For example, 36% of respondents with an annual household income exceeding £100,000 knew what a connected place was, compared with 19% of those with an annual household income of less than £25,000.

4.1.1 Awareness of connected places or smart city technology

Respondents were also asked whether they had seen examples of connected places or smart city technology being used or developed in their area. Examples of connected places technology include smart lamp posts which control light via sensors, smart bins, and data driven traffic management to improve air quality.

Across all age groups, over half of survey respondents stated that they had not seen any examples of connected places technology, and between 10-15% of respondents said they did not know (Figure 49). Over 65s were more likely to report not seeing any examples of connected places technology than 18-24 year olds (78% and 59%, respectively). This finding is consistent with the previous result that older people were less likely to report being aware of what a connected place is.

Figure 49 Percentage of respondents who had seen examples of connected places or smart city technology, by age group



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

4.2 Attitudes towards connected places or smart city technology

4.2.1 Trust in different types of connected places or smart city technology

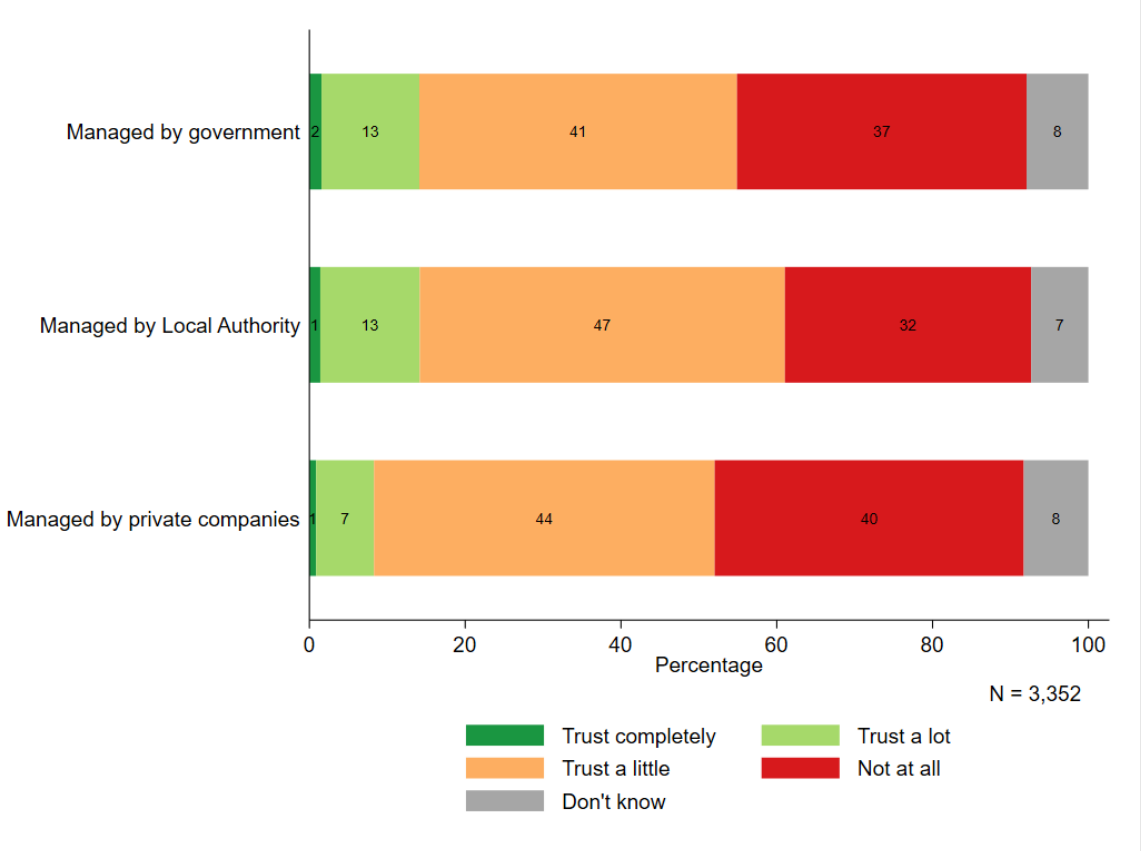
Trust in connected places technology by managing institution

Survey respondents were asked to state the extent to which they would trust different types of connected places technology. Figure 50 shows the extent to which respondents would trust technology managed by different institutions – namely government, Local Authorities, and private companies.

Across all types of institution, respondents were more likely to distrust than trust the technology. Respondents were more likely to 'trust completely' or 'trust a lot' technology managed by government (15%) or Local Authorities (14%) than technology managed by private companies (8%).

Regardless of the institution, respondents with a lower household income were more likely to state they did not trust the technology at all. For example, 42% of respondents with a household income of less than £25,000 said they would not trust technology managed by the government, compared to 21% of respondents with a household income greater than £100,000.

Figure 50 Extent to which respondents trust different types of smart technology, by institution responsible for managing the technology



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

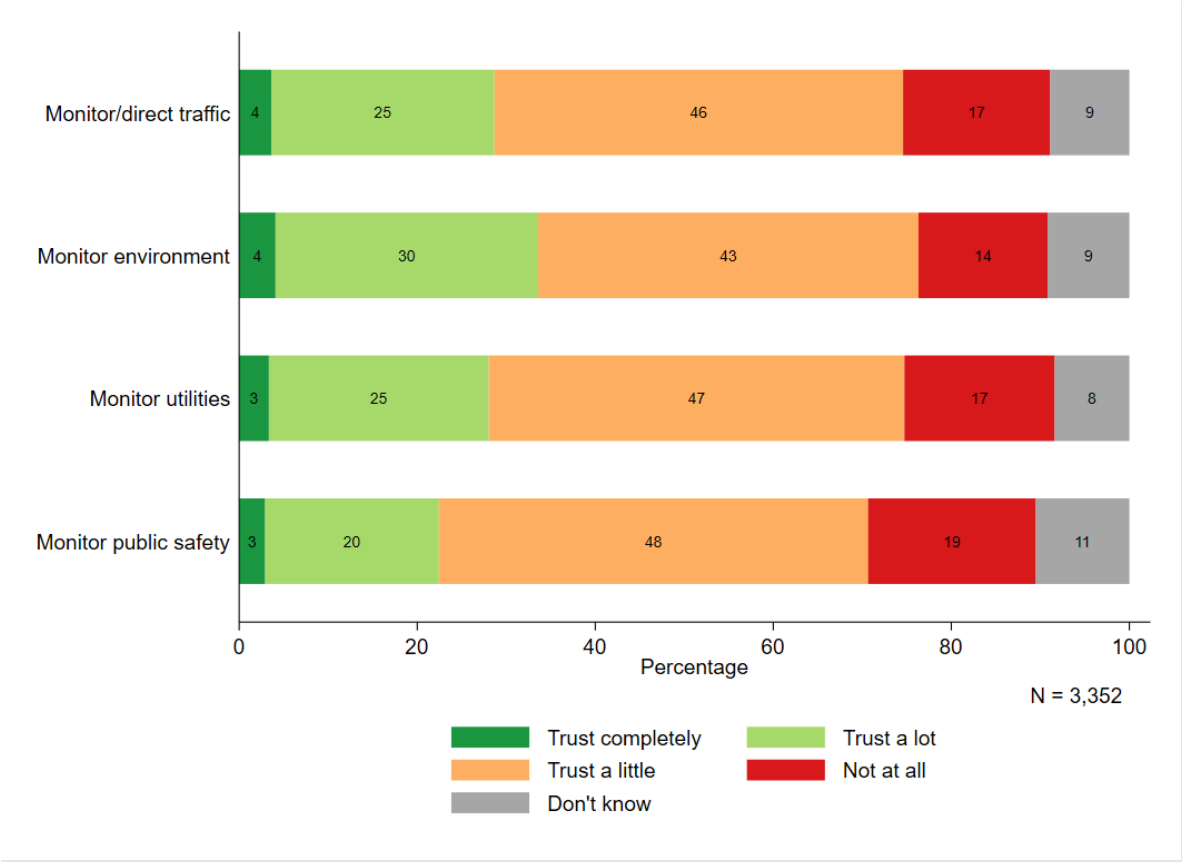
Source: London Economics/YouGov

Trust in connected places technology across different use functions

Connected places can be used for a range of different functions, for example environmental monitoring such as sensors to monitor water levels or smart traffic management that reduce congestion on busy roads. Respondents were asked to state the extent to which they trusted connected places technology across different usage types. As shown in Figure 51, stated levels of trust were relatively consistent across usages.

As with different managing institutions, most respondents indicated that they either trusted a little or did not trust connected places technology at all. For example, only 23% of respondents stated that they 'trusted completely' or 'trusted a lot' technology to monitor public safety.

Figure 51 Extent to which respondents trust different types of smart technology, by usage of the technology



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

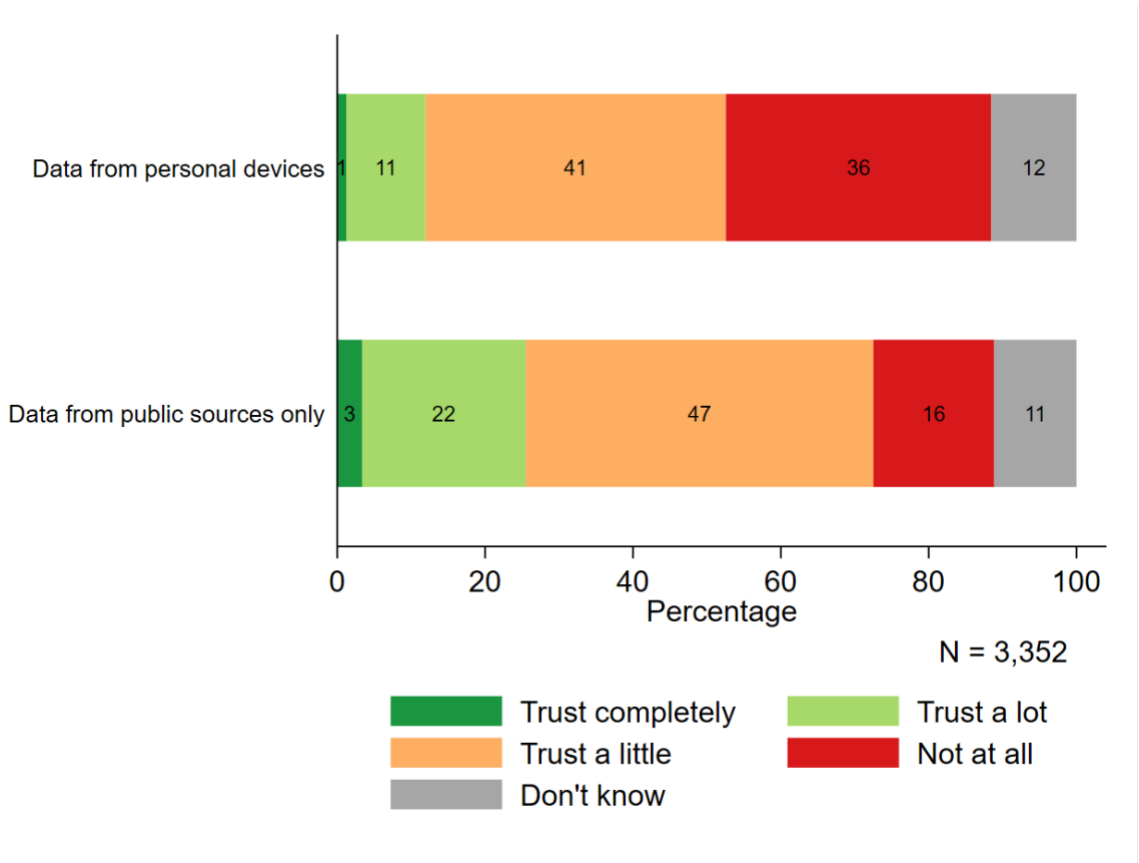
Source: London Economics/YouGov

Trust in connected places technology across different data requirements of the technology

Lastly, survey respondents were asked to state the extent to which they trusted connected places technology by different levels of data requirement – specifically whether the technology relied on data from consumer's personal devices or from public information only (e.g. traffic sensors). The results suggest that respondents were less trusting of technology which gathers data from personal devices than technology that leverages only public information (Figure 52).

Only 12% of respondents said they 'trusted completely' or 'trusted a lot' technology which gathered data from personal devices, compared to 25% for that using only public information.

Figure 52 Extent to which respondents trust different types of smart technology, by the type of data used by the technology



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

4.2.2 The extent to which people are concerned about the security of connected places

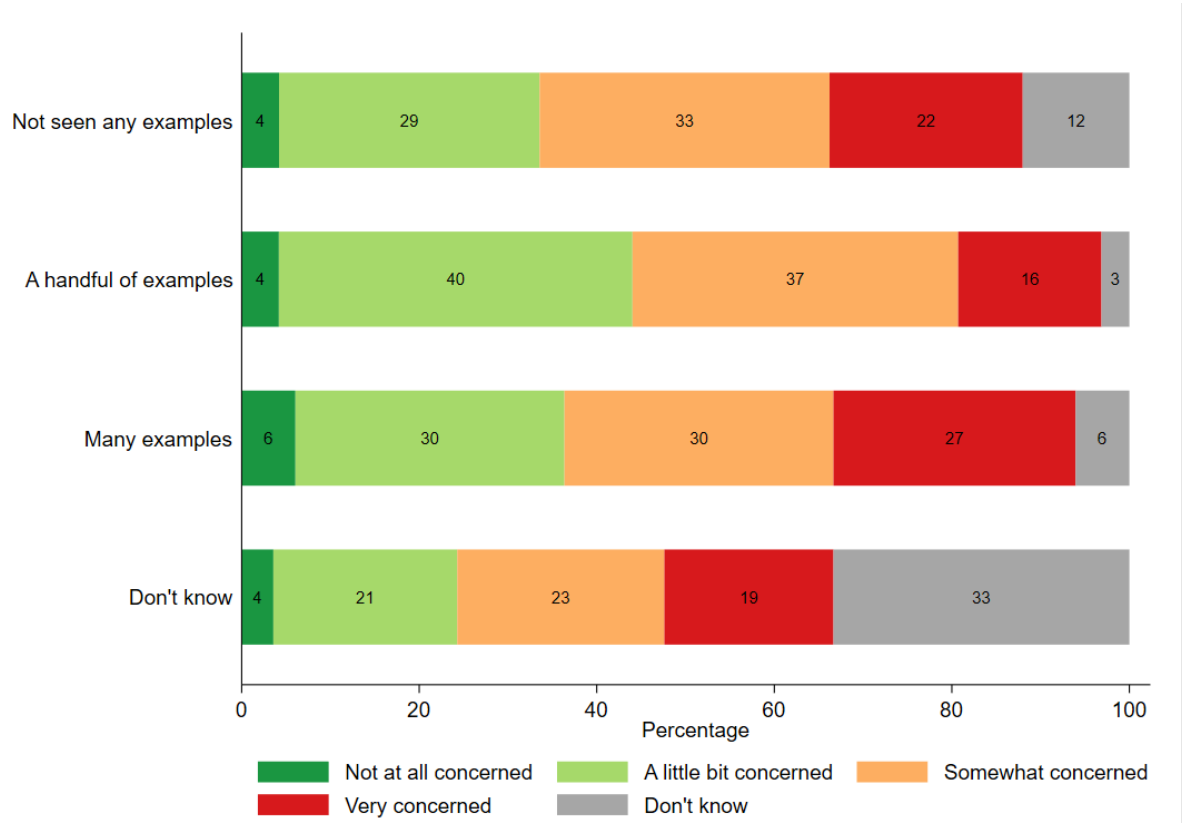
The results in Sections 0 and 4.2.1 suggest that most people are unaware of what connected places are, but that a significant proportion of people would not trust connected places technology across a range of contexts and managing institutions.

It is therefore of interest to understand if awareness and familiarity with connected places or smart city technology mediates concerns about the security of this technology. The link between awareness of connected places or smart cities and level of concern about the security of connected places technology is shown in Figure 53.

The relationship between level of awareness of connected places technology and level of concern about the security of connected places is unclear. The proportion of survey respondents who reported being 'somewhat concerned' or 'very concerned' about security of connected places was similar for respondents who had not seen any examples of smart cities (55%), those who had seen a handful of examples (53%), and those who had seen many examples (57%).

Across these groups, few respondents reported that they were 'not at all concerned' about the security of connected places (ranging from 4% for those who had not seen any examples to 6% for those who had seen many examples).

Figure 53 Level of concern about connected places, by number of examples of connected places technology seen



Note: The chart uses the weighted sample base.

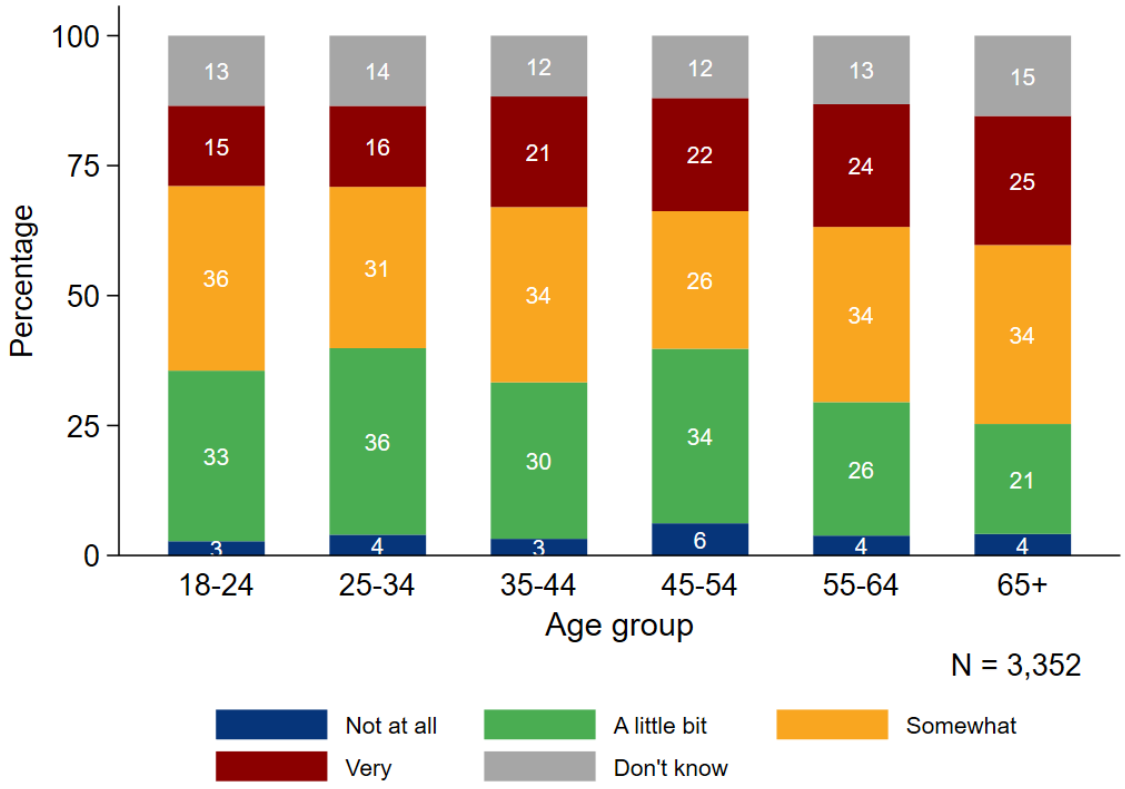
Source: London Economics/YouGov

Demographic differences in level of concern about security of connected places

Figure 54 displays the extent to which survey respondents reported that they would be concerned with the security of connected places or smart cities by age group. Across all age groups few respondents stated that they would not be at all concerned with the security of connected places.

Respondents aged over 65 years old were more likely to state that they were 'very' concerned with the security of connected places (25%), compared to 18-24 year olds (15%). Despite differences in awareness of connected places across household income, there were no systematic differences in the level of concern about the security of connected places.

Figure 54 Level of concern about security of connected places, by age



Note: The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.

Source: London Economics/YouGov

Index of Tables, Figures and Boxes

Tables

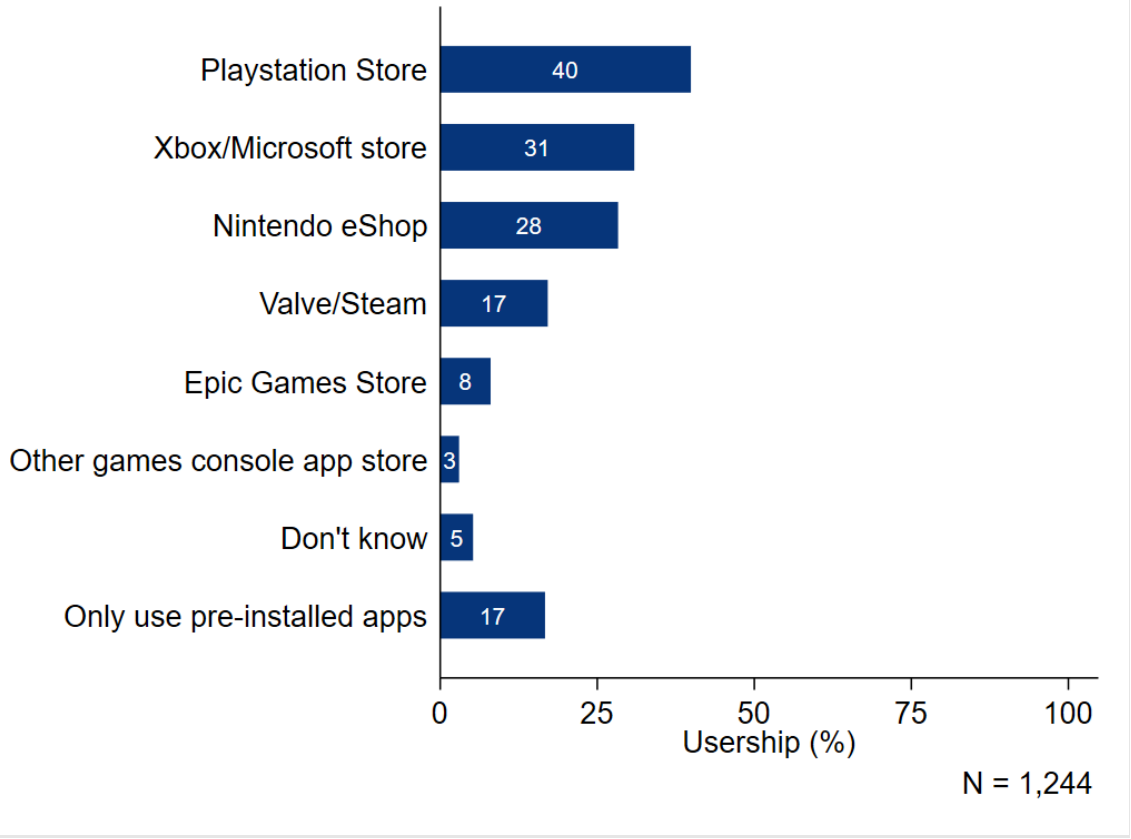
Figures

ANNEXES

Annex 1 App store survey (supplementary results)

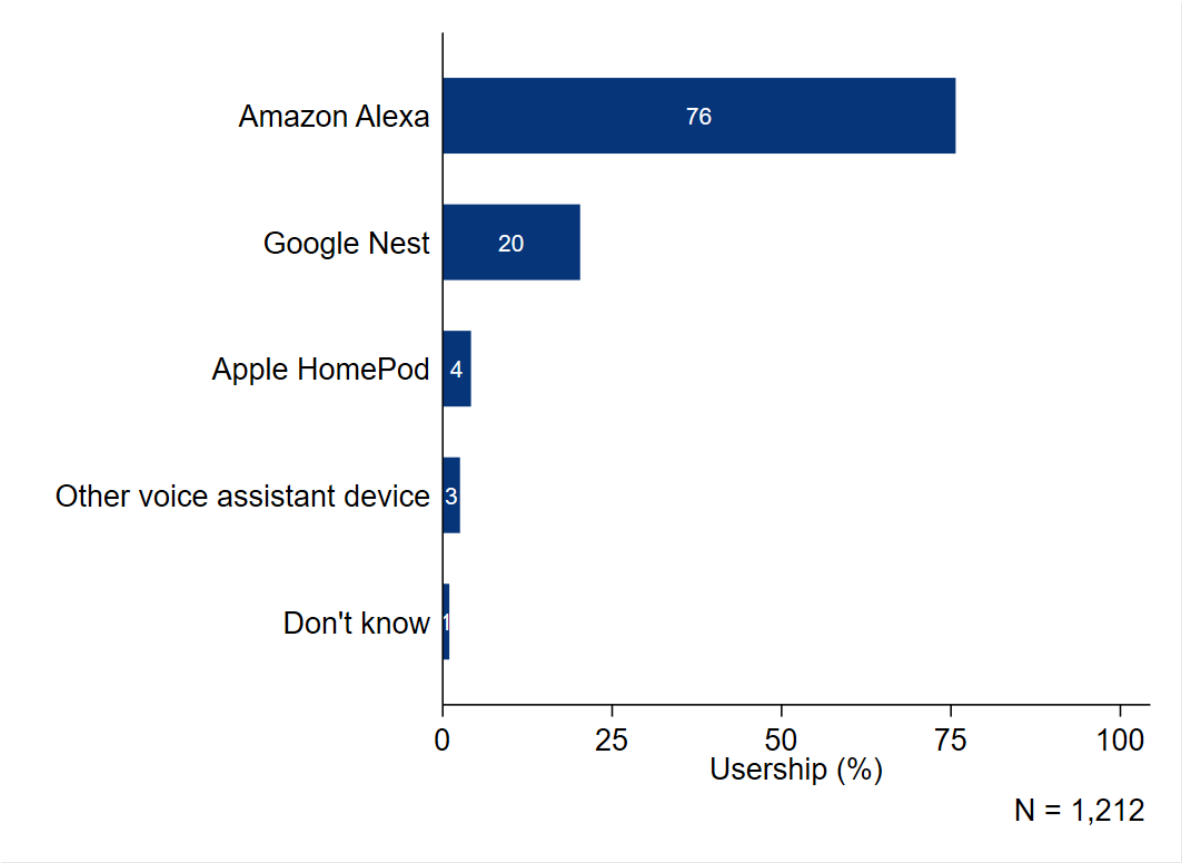
4.3 App store usage

Figure 55 Usage of different games console app stores (% of respondents)



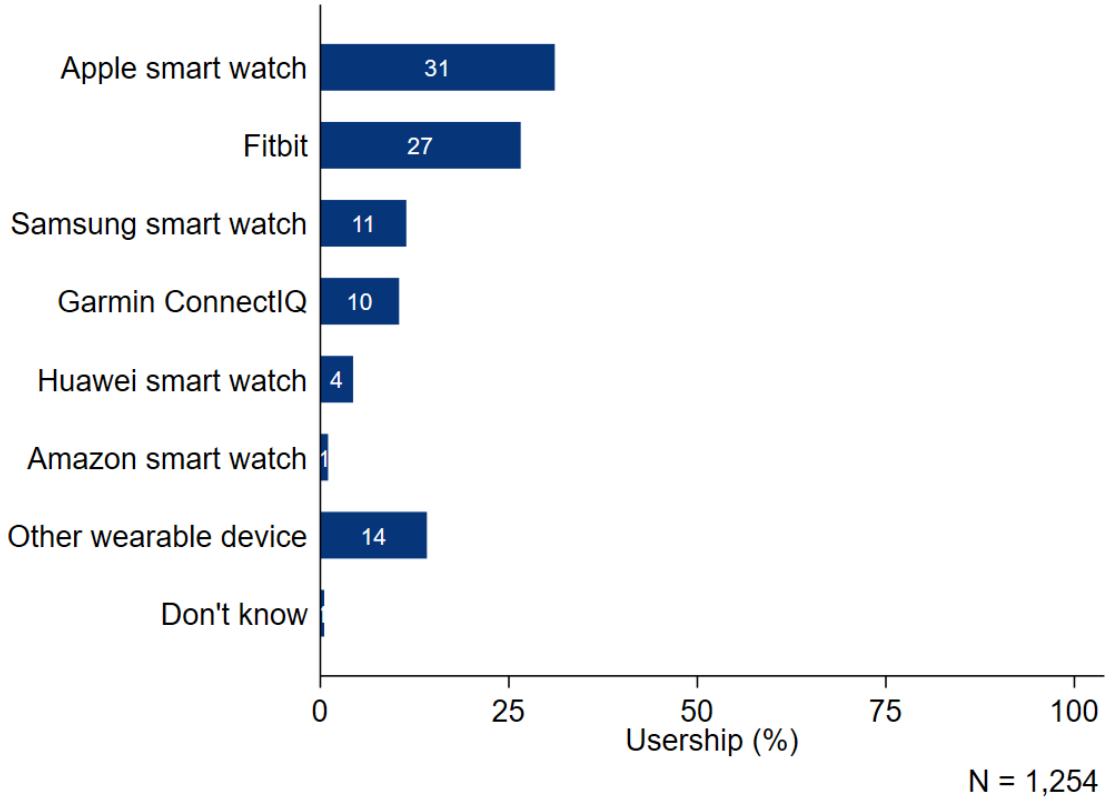
Note: The above figure shows the percentage of respondents who responded that they used a given app store on their games console. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

Figure 56 Usage of different voice assistant app stores (% of respondents)



Note: The above figure shows the percentage of respondents who responded that they used a given app store on their voice assistant device. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

Figure 57 Usage of different wearable device app stores (% of respondents)

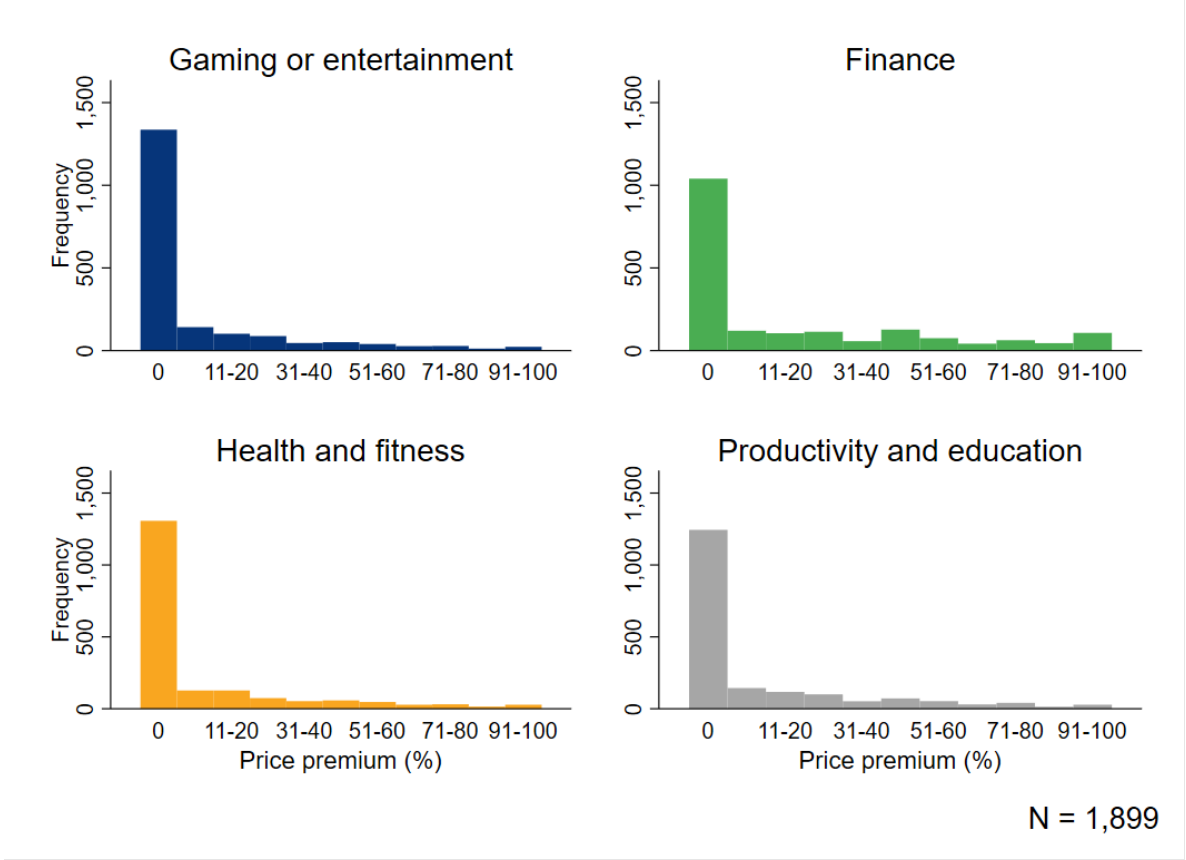


Note: The above figure shows the percentage of respondents who responded that they used a given app store on their wearable device. The chart uses the weighted sample base. The sample size N is shown in the bottom righthand corner.
Source: London Economics/YouGov

Annex 2 Willingness to pay for 50% improvement in security

Figure 58 shows the distribution of consumer willingness to pay for a 50% improvement in app security.

Figure 58 Consumer willingness to pay for 50% improvement in app security, by app type

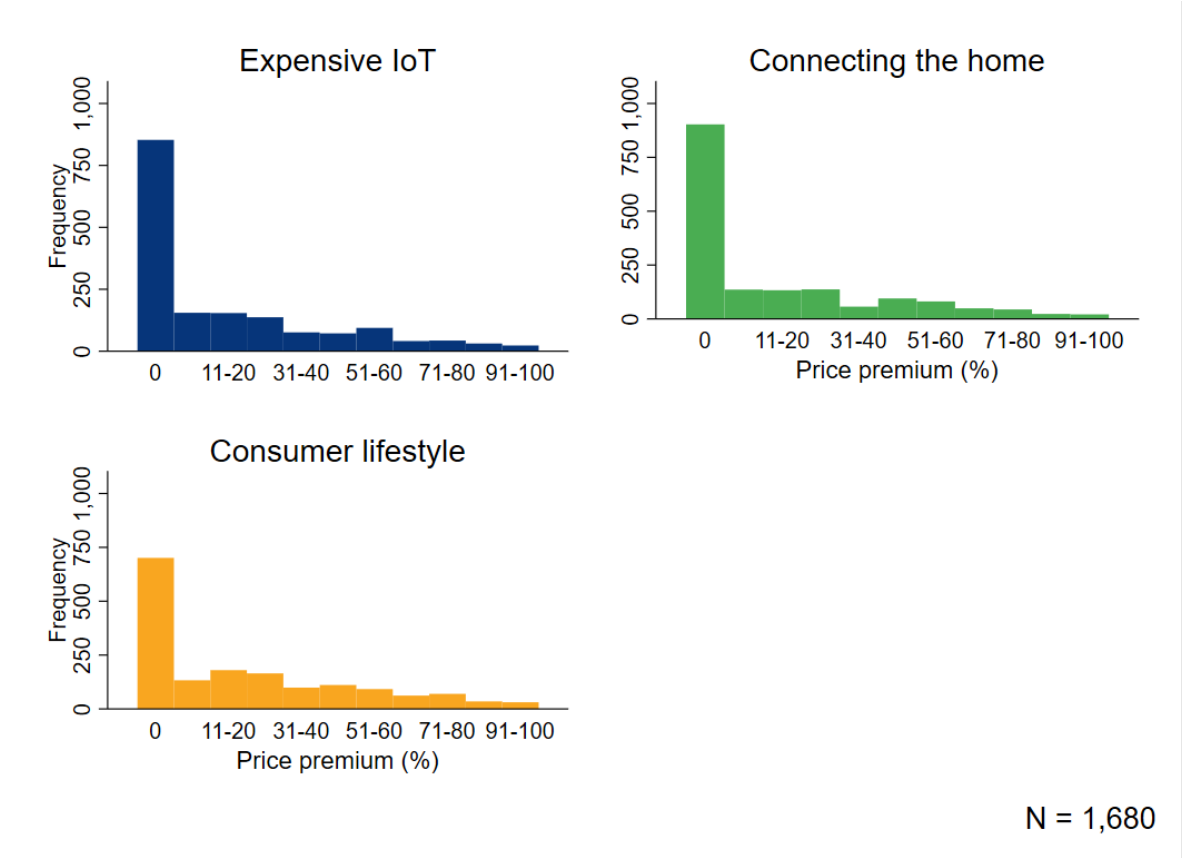


Note: The figure above shows the distribution of respondents' willingness to pay for enhanced security of different categories of app. Enhanced security is measured as a 50% reduction in the number of security incidents experienced each year. Respondents were asked to indicate the percentage premium (from 0-100%) they would be willing to pay for the specified reduction in security incidents. Each bar shows the number of respondents selecting a percentage premium within the bar range. Each bar specifies a range of 10 percentage points except the first bar, which counts the number of respondents selecting 0% (or 'I wouldn't pay anything more').

Source: London Economics/YouGov

Figure 59 shows the distribution of consumer willingness to pay for a 50% improvement in IoT device security.

Figure 59 Consumer willingness to pay for 50% improvement in device security, by device type



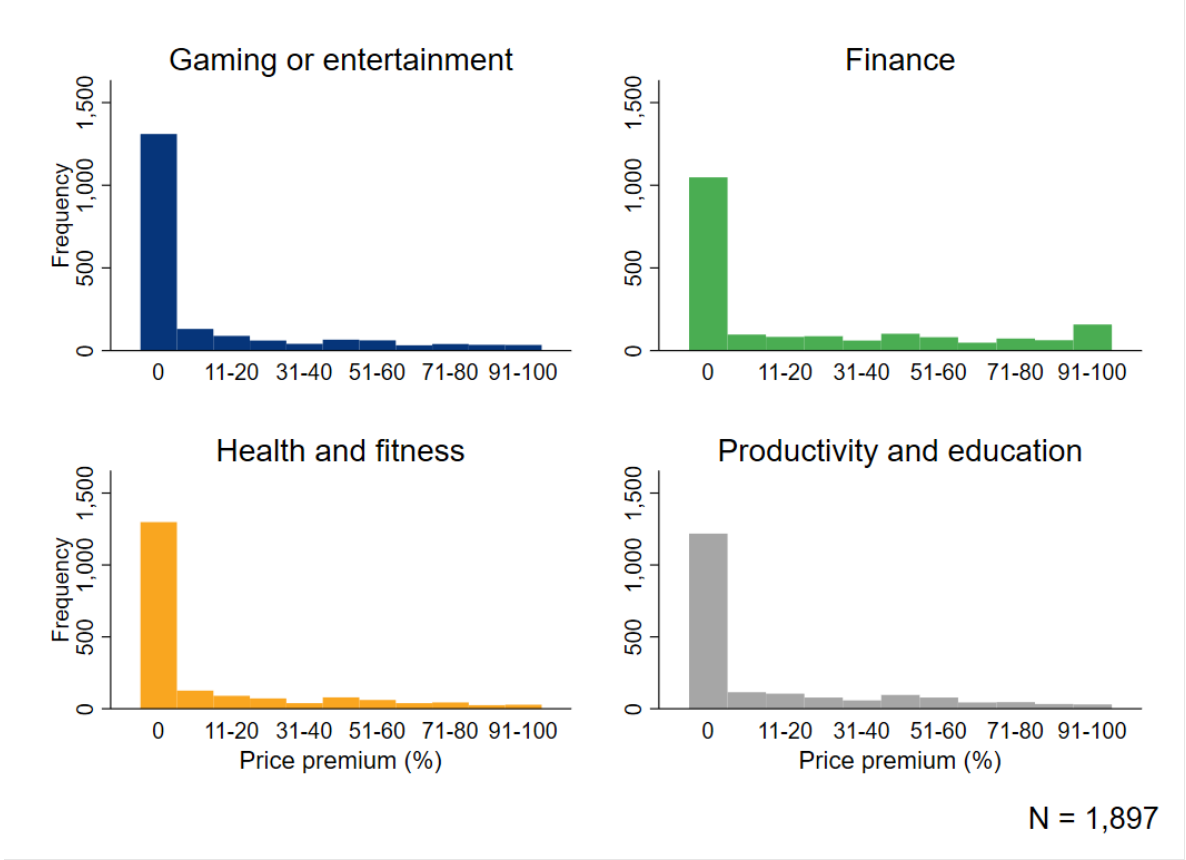
Note: The figure above shows the distribution of respondents' willingness to pay for enhanced security of different types of IoT device. Enhanced security is measured as a 50% reduction in the number of security incidents experienced each year. Respondents were asked to indicate the percentage premium (from 0-100%) they would be willing to pay for the specified reduction in security incidents. Each bar shows the number of respondents selecting a percentage premium within the bar range. Each bar specifies a range of 10 percentage points except the first bar, which counts the number of respondents selecting 0% (or 'I wouldn't pay anything more').

Source: London Economics/YouGov

Annex 3 Willingness to pay for 90% improvement in security

Figure 60 shows the distribution of willingness to pay for a 90% improvement in app security.

Figure 60 Consumer willingness to pay for 90% improvement in app security, by app type

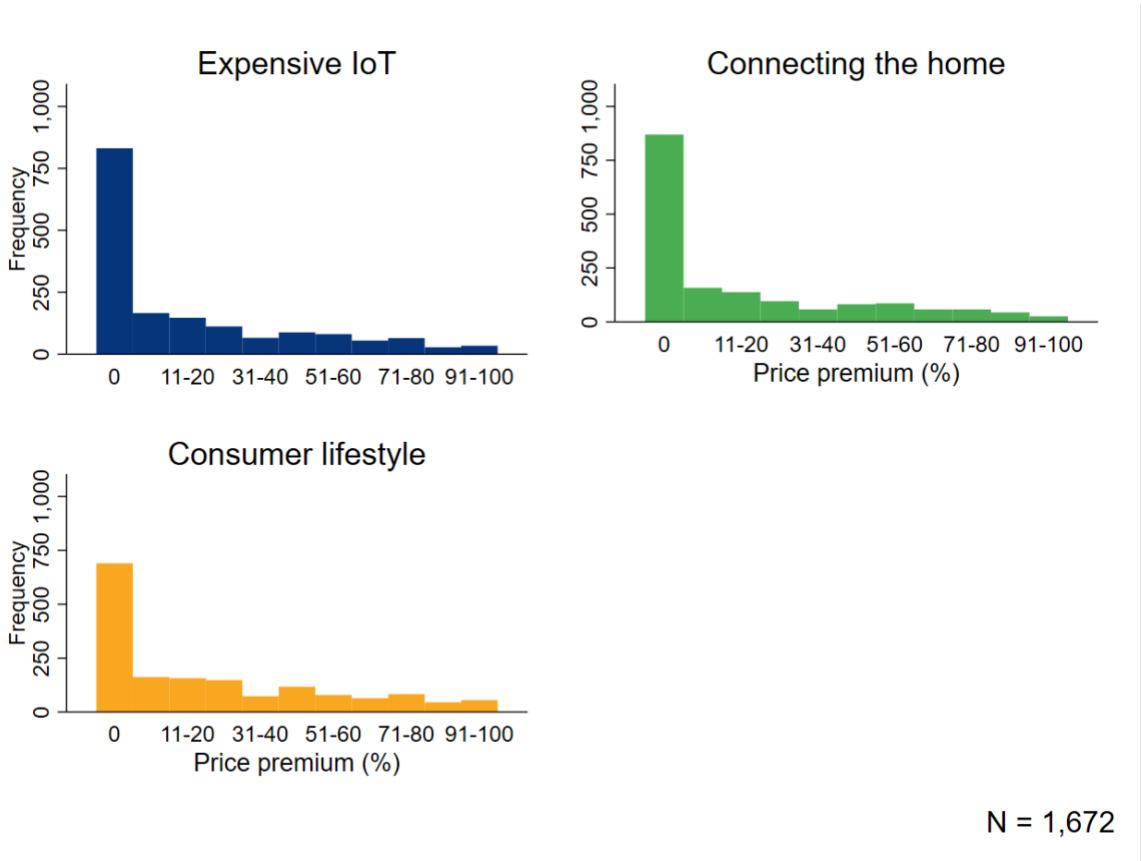


Note: The figure above shows the distribution of respondents' willingness to pay for enhanced security of different categories of app. Enhanced security is measured as a 90% reduction in the number of security incidents experienced each year. Respondents were asked to indicate the percentage premium (from 0-100%) they would be willing to pay for the specified reduction in security incidents. Each bar shows the number of respondents selecting a percentage premium within the bar range. Each bar specifies a range of 10 percentage points except the first bar, which counts the number of respondents selecting 0% (or 'I wouldn't pay anything more').

Source: London Economics/YouGov

Figure 61 shows the distribution of willingness to pay for a 90% improvement in IoT device security.

Figure 61 Consumer willingness to pay for 90% improvement in device security, by device type



Note: The figure above shows the distribution of respondents' willingness to pay for enhanced security of different types of IoT device. Enhanced security is measured as a 90% reduction in the number of security incidents experienced each year. Respondents were asked to indicate the percentage premium (from 0-100%) they would be willing to pay for the specified reduction in security incidents. Each bar shows the number of respondents selecting a percentage premium within the bar range. Each bar specifies a range of 10 percentage points except the first bar, which counts the number of respondents selecting 0% (or 'I wouldn't pay anything more').

Source: London Economics/YouGov

Annex 4 Supporting data for Figure 1 (personal and household ownership of consumer IoT devices)

Device type	Personal ownership	Household ownership
Connected children's toys	2%	4%
Smart baby monitors	3%	3%
Smart TVs	64%	23%
Smart speakers	38%	18%
Wearable health trackers/smart watches	37%	26%
Smart home thermostats	16%	8%
Smart lighting	15%	7%
Smart doorbells	14%	7%
Smart video cameras	12%	6%
Smart smoke detectors	7%	4%
Smart washing machines	8%	4%
Smart fridges	3%	3%
Smart ovens	2%	2%
Smart microwaves	2%	2%
Tablets	53%	36%
Laptops	69%	38%
Smart pet products	2%	1%
Connected garden devices	3%	2%
Smartphones	92%	54%
Other	9%	6%
N	*3352*	*3352*

Annex 5 Supporting data for Figure 6 (frequency of upgrading, replacing, or disposing of consumer IoT device, by device group)

Table 4 Percentage of respondents indicating different frequencies of upgrading, replacing, or disposing consumer IoT devices, by device type

Frequency of upgrading, replacing, or disposing	IoT device type		
	Expensive	Connecting the home	Consumer lifestyle
Every 6 months or more often	2%	3%	1%
Every 6 months to 1 year	3%	8%	1%
Every 1 or 2 years	4%	16%	15%
Every 2 to 5 years	28%	34%	63%
Every 5 to 10 years	43%	18%	12%
Less frequently than every 10 years	9%	6%	2%
Not applicable	2%	3%	1%
Don't know	9%	11%	4%
N	*701*	*440*	*1742*

Source: London Economics/YouGov.

LE London Economics

Somerset House, New Wing, Strand,
London, WC2R 1LA, United Kingdom
info@londoneconomics.co.uk
londoneconomics.co.uk
@LondonEconomics
+44 (0)20 3701 7700