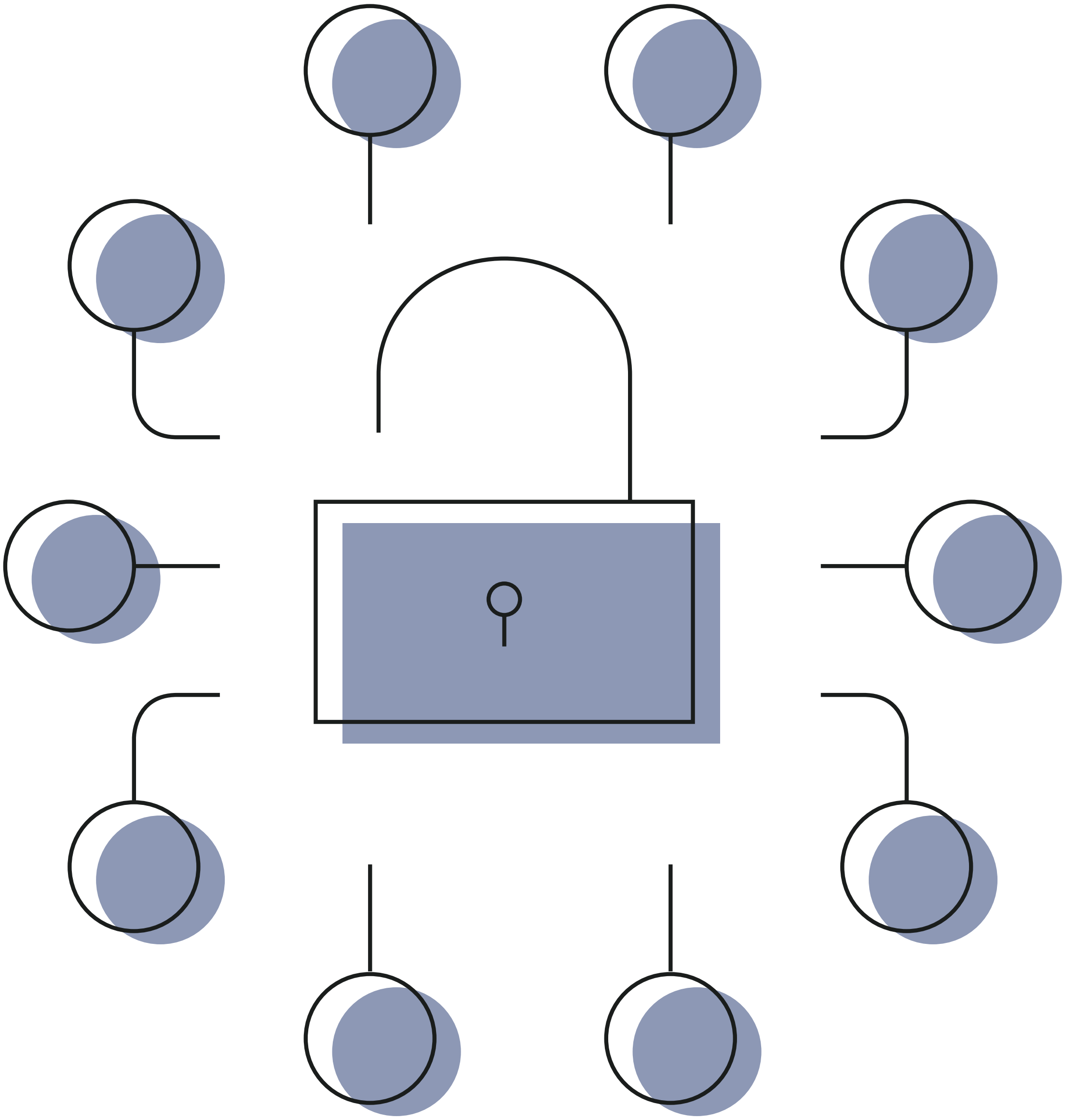
The Economist INTELLIGENCE UNIT

A report from The Economist Intelligence Unit

# What the Internet of Things means for consumer privacy



Sponsored by FORGEROCK

# Contents

# About this report

*What the Internet of Things means for consumer privacy* discusses the findings of an Economist Intelligence Unit (EIU) research programme, sponsored by ForgeRock, that explores the privacy concerns and priorities of global consumers stemming from the Internet of Things (IoT) and related technologies.

At the core of the research is a global survey of 1,629 consumers that The EIU conducted in October 2017. Respondents come from eight countries: Australia, China, France, Germany, Japan, South Korea, the UK and the US. They fall into six age groups ranging from 16 to over 65, and the sample is divided evenly among men and women.

Additional insights were obtained from in-depth interviews with experts on privacy in the digital era. Our thanks are due to the following individuals:

- Giulio Coraggio, partner, head of global IoT and gaming, DLA Piper
- Amanda Long, director-general, Consumers International
- Kathleen McGee, head, Bureau of Internet and Technology, Office of the Attorney-General of the State of New York

This report was written by Denis McCauley and edited by Veronica Lara from The EIU.

# Introduction

"The IoT combines the technologies of multiple providers, which makes the tracking of collected personal data extremely difficult, if not impossible, in most cases."

Giulio Coraggio,
partner, head of global IoT and gaming, DLA Piper

As the digital era has unfolded, consumers have become steadily more aware of the uses that businesses make of the personal information that is handed over when accessing services. Many consumers have become adept at exercising control over how their data are used, for example through consent forms and opt-outs. However, the IoT—the rapidly expanding network of devices, physical objects, services and applications that communicate over the internet—poses a new set of privacy challenges, as it changes the relationship between individuals and their personal data. Gartner, a research firm, projected the number of "connected things" in the global consumer segment to reach 7bn in 2018, rising to 12.9bn in 2020.[1]

The biggest challenges are ubiquity and invisibility: connected devices number in the billions today, and they transmit data without device owners knowing when or how that happens. "American consumers are very knowledgeable about privacy protection issues," says Kathleen McGee, head of the Bureau of Internet and Technology at the New York State Attorney-General's office, "but they do not appreciate just how far-reaching IoT devices are in their world."

The data custody chains, or documentation recording the transfer of data to different parties, are also complex. "The IoT combines the technologies of multiple providers, which makes the tracking of collected personal data extremely difficult, if not impossible, in most cases," says Giulio Coraggio, partner and head of global IoT and gaming at DLA Piper, a law firm.

The same issues make the privacy challenges of the IoT difficult for government and industry to address. According to Amanda Long, director-general of Consumers International, a consumer advocacy organisation headquartered in London, it is the cross-sector and crossborder interlinkages that make the IoT such a tricky area for stakeholders to grasp and address.

A handful of organisations are seeking to build consumer and industry knowledge about the unique challenges the IoT poses to data privacy. These include non-governmental organisations (NGOs) such as Consumers International and the Online Trust Alliance (OTA).[2] Government bodies such as the UK's Information Commissioner's Office and the US Federal Trade Commission (FTC), and inter-governmental organisations such as the Global

[1] Gartner, February 7th 2017. "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016," https://www.gartner.com/newsroom/id/3598917

[2] The OTA is part of the Internet Society, a US-based non-profit organisation that seeks to foster common practices and standards for internet infrastructure and use.

Privacy Enforcement Network (GPEN), are also prominent in such efforts.[3]

The purpose of this report is to augment the discussion by identifying consumers' main privacy concerns in relation to internet-connected devices. To explore this topic, The EIU has conducted a survey of over 1,600 consumers in eight countries. The report draws on the analysis of the results and discusses how industry and government can help to build consumer trust in the age of IoT. ■

[3] The GPEN is an inter-governmental committee of privacy enforcement authorities.

# 1 A perception of danger

> "A growing number of people are connected to the smart grid, for example, and they don't have a choice about transmission of their data."
>
> Amanda Long,
> director-general,
> Consumers International

Consumers may not appreciate the ubiquity of interconnected sensors in their everyday devices, but they nonetheless sense danger about the automatic transmission of their personal data. This is supported by the fact that consumers' perceptions of risk maps closely to the activities in which they most often use internet-connected devices. For example, consumers' two most frequently reported uses of connected devices (eg, smartphones and laptops) are to make online payments for goods and services, and to access personal messaging and social networks—with each of these activities cited by approximately 80% of respondents. These activities are also the two most commonly perceived as riskiest, with 79% of survey respondents believing online payments put personal privacy at least "somewhat at risk", and 74% saying so for messaging and social networks.

This may explain why consumers value the security (80% assessing this as "very important") and privacy (75%) features of devices much more highly than the devices' affordability (47%) or ease of use (48%). It is no surprise to Mr Coraggio, who notes that consumers are well aware that their data have been commodified by companies. Respondents' concern with this resounds clearly in the survey, where 89% cite their discomfort with the ability of third parties to access personal data without their consent. Nine in ten fear the possibility of identity theft or fraud, and nearly as many believe their personal data may not be secure in the hands of online service providers and device manufacturers.

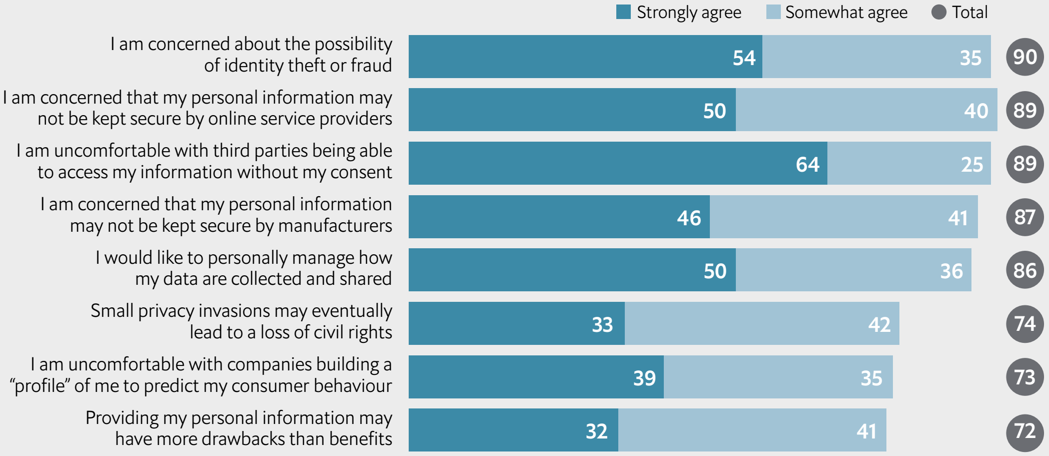
Consent, or the lack of it, looms large in consumer fears about how their data are being used. For Ms Long, the main issue is the lack of choice involved in the automatic collection and transmission of data inherent in the IoT: "A growing number of people are connected to the smart grid, for example, and they don't have a choice about transmission of their data." Ms McGee notes that although many consumers concerned about privacy exercise choice by declining to purchase some smart home appliances, say for the kitchen, they may be less aware that other devices, such as their televisions, are collecting data about their habits and preferences. Even when they are fully aware, they may not be given the choice of opting out, as in the case, cited by Ms Long, of a national rollout of smart meters to every energy user.

Consumer concerns are about more than material damage resulting from such collection and sharing of their data without consent. About three of every four respondents (74%) fear that cumulative privacy invasions could weaken their civil rights. Such fears are not misplaced: a 2016 report from the US FTC acknowledged the potential that "big data" could be used to support discriminatory practices by businesses and governments.[4]

[4] Federal Trade Commission, January 2016, *Big Data: A Tool for Inclusion or Exclusion?*, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

## To what extent do you agree or disagree with the following statements?

(% of respondents)



Note: Percentages may not add to total due to rounding.

Source: Economist Intelligence Unit survey, 2018.

On a regional level, the US consumers surveyed are the most wary of data misuse: 76% are strongly concerned with third parties accessing their information without consent, compared with 68% in Europe and 57% in the Asia-Pacific (APAC) region. Compared with other regions, US respondents most frequently cite strong concern with the building of behavioural profiles based on their data, and the potential of identity theft and fraud resulting from security breaches.

Data privacy has become a "hot button" issue for US consumers in the past couple of years, according to Ms McGee. "They should be concerned with what corporate America and government alike are doing in their bedrooms," she says. "I would like to see a lot more transparency about how personal data are being collected and used." ■

## 2 Control and transparency

What could assuage the data privacy fears that consumers have voiced? The survey provides some clues.

Nearly nine in ten respondents (86%) want the ability to manage their personal information proactively. And many would value the creation of channels (such as unsubscribe platforms and personal user profiles) to ensure their personal information is kept private. When it comes to the automatic collection of data, consumers want the power to control what personal information is collected by connected devices—92% say this is important, including about two of every three saying it's "very important". The overwhelming majority also demand transparency about automatic data collection, which means being informed when personal data are being collected (92%), and being notified at the point of sale about the data collection capabilities of devices (89%).

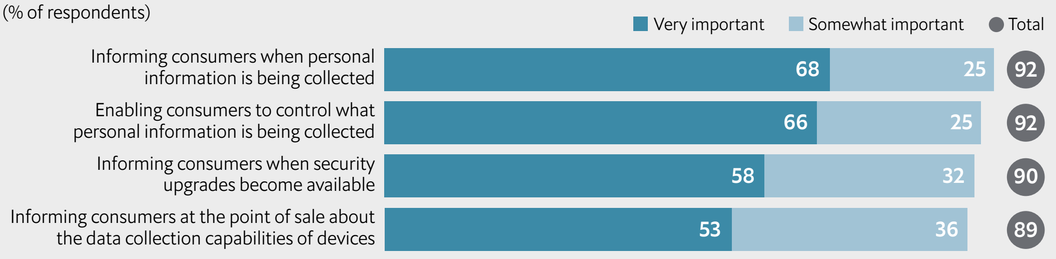
However, the reality is that consumers are today providing much—if not most—of their data through such devices involuntarily and without any clarity. A 2016 GPEN study found that six of every ten IoT devices did not properly inform consumers about how their personal data are being used, and 72% did not instruct consumers how to delete their data from the device.[5] "Whether consciously or not, consumers are paying for the use of free applications and services with their data," says Mr Coraggio.

The demands from consumers in our survey raise the question of how much consumer control of IoT-enabled data transmission is actually realistic. "Control is almost impossible when you don't have transparency or choice," says Ms McGee. "I'm sure I cross the paths of many IoT sensors every time I walk out to get a coffee," she observes. "I have no control over that and I have no transparency."

Consumers say they want control over their automatically transmitted data, believes Ms Long, probably because they currently have very little.

**How important are each of the following actions in terms of protecting the personal information consumers provide for automatic collection?**

(% of respondents)



Note: Percentages may not add to total due to rounding.

Source: Economist Intelligence Unit survey, 2018.

[5] Global Privacy Enforcement Network, *2016 GPEN Annual Report*, https://www.privacyenforcement.net/sites/default/files/Annual%20Report%202016.pdf

There are not many examples of good data control tools in the IoT market, and companies that recognise this absence ought to be able to begin taking measures to provide some degree of control. She says: "There's a gap in the market for a smart business to try to do this." The dilemma, according to Ms Long, is that no one has yet been able to identify practical forms of direct control for IoT devices.

Because of these difficulties, solutions are more likely to coalesce around transparency, in the view of Ms McGee. This, she maintains, is where regulators are going to channel their privacy demands toward industry in relation to the IoT. "From a regulatory perspective, in the US we are going to expect clear terms and conditions and transparency in terms of use of data, and we will be enforcing them." But that raises another difficulty, relating to the often long chain of data custody. "We need to determine how many steps from origin are required in terms of transparency," she says, "as consumer data collected in this way change hands many, many times."

""We need to determine how many steps from origin are required in terms of transparency..."

Kathleen McGee, head of the Bureau of Internet and Technology, Office of the Attorney-General of the State of New York

What will regulators use to guide such determinations? When it comes to IoT privacy risks specifically, discussions tend to revolve around the development of standards rather than new legislation. Mr Coraggio believes the legal safeguards being built now for data privacy, at least in Europe through the EU's General Data Protection Regulation (GDPR), are adequate to deal with IoT-specific risks. "GDPR is very strict," he says.

Scheduled to enter into force in May 2018, GDPR is the world's most comprehensive effort to date to bring countries' data protection rules into line with the modern capabilities of digital technology. Its impact will be felt far beyond Europe and, as we will see, it is already shaping consumer attitudes about their rights to data privacy. ■

# 3 Consumer demands for privacy rights

GDPR is going to have a spill over effect in the US.

Judging by the survey, many consumers globally want the types of data privacy rights that EU citizens will enjoy when GDPR comes into force. When asked to cite the most important rights regarding third-party use of their personal information, the majority of consumers (57%) most frequently cite the right to erasure of their information (also known as "the right to be forgotten"), followed by the rights to object to the use of their personal data, and to be informed in a clear way how the data are being used.

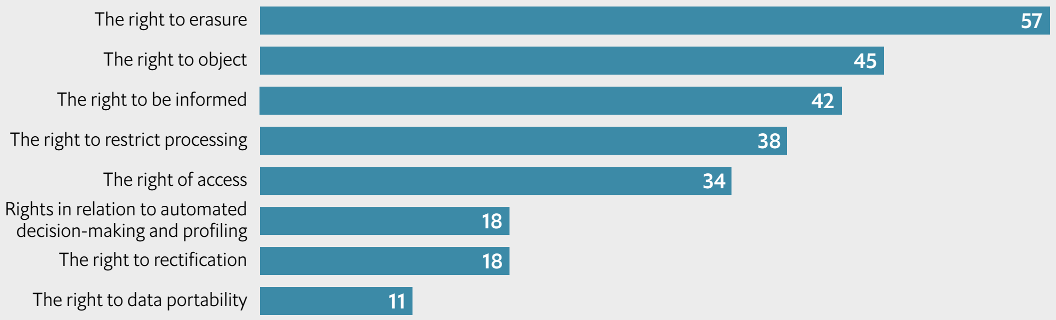
On a regional level, the right to erasure is most frequently cited by European consumers (61%), and it remains at the top of consumers' lists in APAC (56%) and the US (50%). Demand for the right to object is weaker, however, in APAC (39%) than in Europe or the US (50% in each). Notwithstanding these few differences, consumers in all three regions place the greatest weight on those rights that address fundamental issues of transparency and control.

The enumerated rights mirror those enshrined in GDPR, and although none are specific to the challenges raised by the IoT, they are directly relevant to it. According to Mr Coraggio: "GDPR grants individuals much stronger tools, such as the [ability to launch class action claims] against companies that exploit consumers' personal data."

Ms Long agrees that IoT-relevant privacy prescriptions are well enshrined in GDPR, and points out that they apply to all companies that process EU citizens' data. Many US and Asian companies, then, whether or not they have a physical EU presence, will need to abide by GDPR.

The worldwide influence of the new EU rules may also come to be felt by non-EU consumers. For example, Ms McGee believes GDPR is going to have a spill over effect in the US. "American regulators and consumers are starting to have a new construct of what privacy means and what consent means. It's shifting towards a European model." ■

**Thinking about your personal information and how it might be used by third parties, which of the following rights do you consider most important? Please select up to three.**
(% of respondents)



Source: Economist Intelligence Unit survey, 2018.

# 4 What industry and government can do

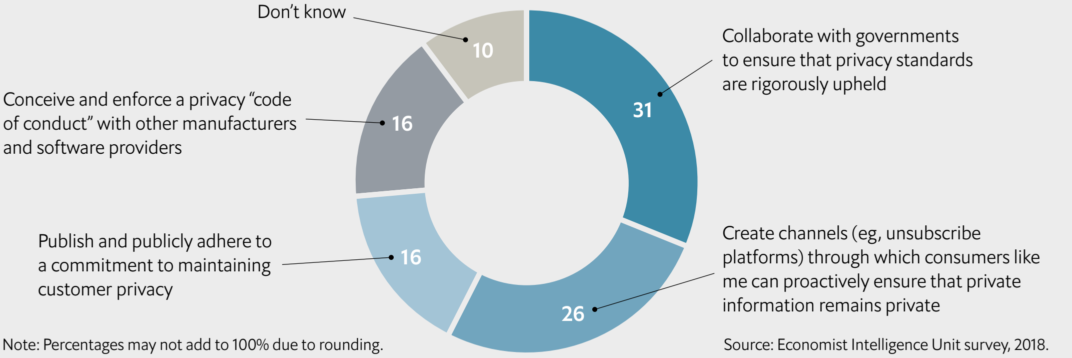
If proactive consumer management of their personal data proves to be impractical in the IoT context, confidence building measures in the IoT's integrity are well within the ability of industry and government. Improved transparency is realistic, according to the experts we interviewed for the study, and is a good starting point for building trust. "If consumers are adequately informed of how their personal data are processed, it should be possible to build their confidence in the IoT," says Mr Coraggio. Efforts such as posting simple notices or electronic alerts that devices are autonomously collecting data are small steps towards building transparency. They could help device manufacturers and service providers improve customer relationships and enhance their brand.

At the very least, some consumers would like such companies to publicly commit to maintaining consumer privacy. Cross-industry standards on delivering such transparency and other privacy protections would also help to earn consumer trust. Nearly a third of respondents say that a rigorously upheld industry-led commitment to privacy protection would be effective, either from individual companies or as a collectively maintained "code of conduct" across industries. A similar share of respondents demand that industry collaborate with governments to develop privacy standards and ensure their rigorous enforcement.

Such rigour, consumers believe, requires sanctions: 92% want stricter punishment than exists today for companies that violate consumer privacy norms. Mr Coraggio agrees: although he believes that GDPR provides sufficient remedies for consumers and governments to address privacy violations, he says that business compliance needs to be monitored more closely than has been the case previously. "Otherwise," he states, "the privacy rules will never be taken seriously."

Enforcement of GDPR rules is the job of each EU

**Which of the following measures would be most likely to make you more confident that your information is being kept private and secure?**
(% of respondents)



Note: Percentages may not add to 100% due to rounding.

Source: Economist Intelligence Unit survey, 2018.

member's supervisory authority, which in most cases is its data protection agency or regulator.[6] The penalties it can apply if a company is found to be in breach are stiff: up to 4% of annual global turnover or €20m (whichever is greater).[7]

According to Ms Long, monitoring and enforcement will not be effective unless countries establish oversight bodies that have responsibility for all aspects of digital consumer protection. Such bodies exist in many countries such as the UK, she says, but few operate with the scope necessary to address the full range of challenges posed by digital technologies.[8]

Voluntary standards and guidelines agreed by multiple stakeholders would do much to build trust in the IoT but, as Ms Long notes, these typically require leadership from institutions such as the UN, OECD or International Organisation for Standardisation and can often take several years to complete. She points out that the international UN guidelines on consumer protection include some digital elements, particularly related to e-commerce, which can act as a starting point for future development of IoT standards.[9] ■

[6] See, for example, the blog at: PwC, February 15th 2017, "Identifying a controller or processor's lead supervisory authority," http://pwc.blogs.com/data_protection/2017/02/identifying-a-controller-or-processors-lead-supervisory-authority.html

[7] EUGDPR.org, "GDPR Key Changes," https://www.eugdpr.org/key-changes.html

[8] Consumers International, in *Securing Consumer Trust in the Internet of Things: Principles and Recommendations*, makes the following recommendation: "Countries should have oversight bodies with responsibility for all aspects of digital consumer protection including the internet of things. Such bodies must have the necessary authority and independence to fulfil their mandates and the technical resources and capabilities to respond to developments in the sector," http://www.consumersinternational.org/media/154809/iot-principles_v2.pdf

[9] UN Conference on Trade and Development, *United Nations Guidelines for Consumer Protection*, 2016, http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1598

# Conclusion

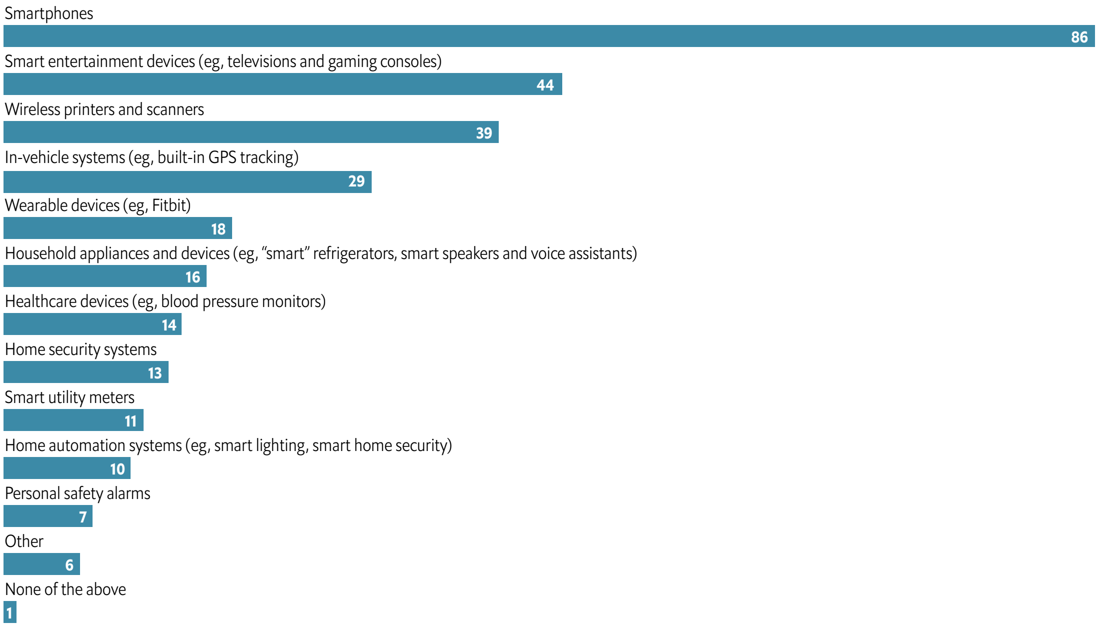
The jury may be out on whether IoT-specific privacy legislation is needed, but experts and consumers appear to agree that GDPR's provisions are a good starting point for countries looking to build concrete privacy safeguards relevant to the IoT. There is also a broad consensus that, along with IoT-related bodies of privacy standards and guidelines, close monitoring is needed to ensure adherence by device manufacturers and service providers. These messages come through clearly from the consumers in our survey and the experts we interviewed.

It is also apparent that more education and knowledge-building efforts are needed by all stakeholders involved, perhaps even before standards are developed. NGOs and a few government bodies have led the way in this effort, but manufacturers and service providers in the IoT value chain need to join in as well. Many have been vocal in discussions on IoT security, but less so when it comes to educating consumers about IoT privacy issues.

Multi-stakeholder agreement of IoT privacy standards is likely to take time, but educational initiatives targeted at both consumers and businesses should be widened, in terms of geography and sectors. Meanwhile, confidence-building measures, such as public company commitments to maintaining privacy or the posting of alerts that devices are collecting data, can be taken by businesses now. The need for such measures is urgent, as the IoT and other data-crunching technologies are moving ahead at great speed. ■

# Appendix: survey results

Percentages may not add to 100% owing to rounding or the ability of respondents to choose multiple responses.

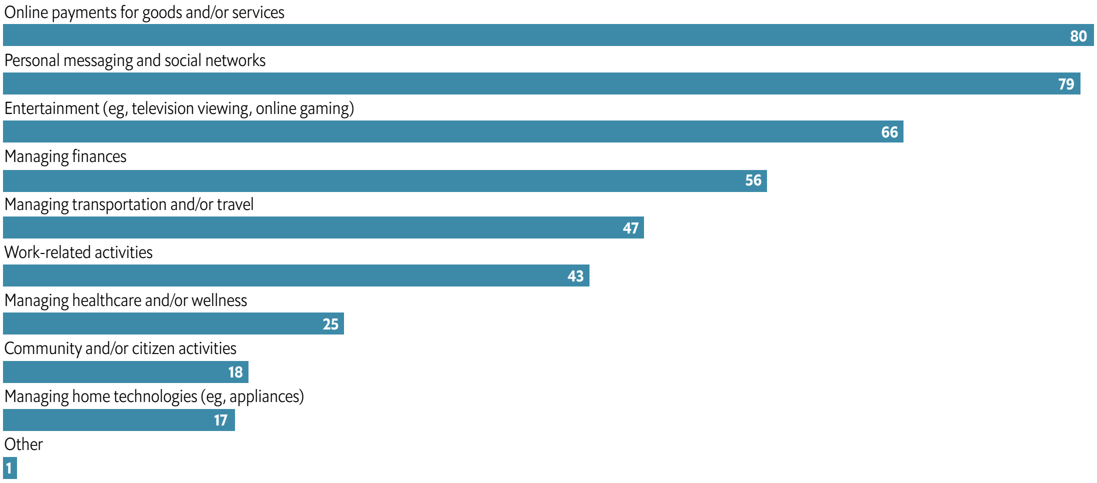


**Which of the following internet-connected devices have you used in the last 12 months?**
Please select all that apply.
(% of respondents)

**For which of the following activities do you use internet-connected devices?**

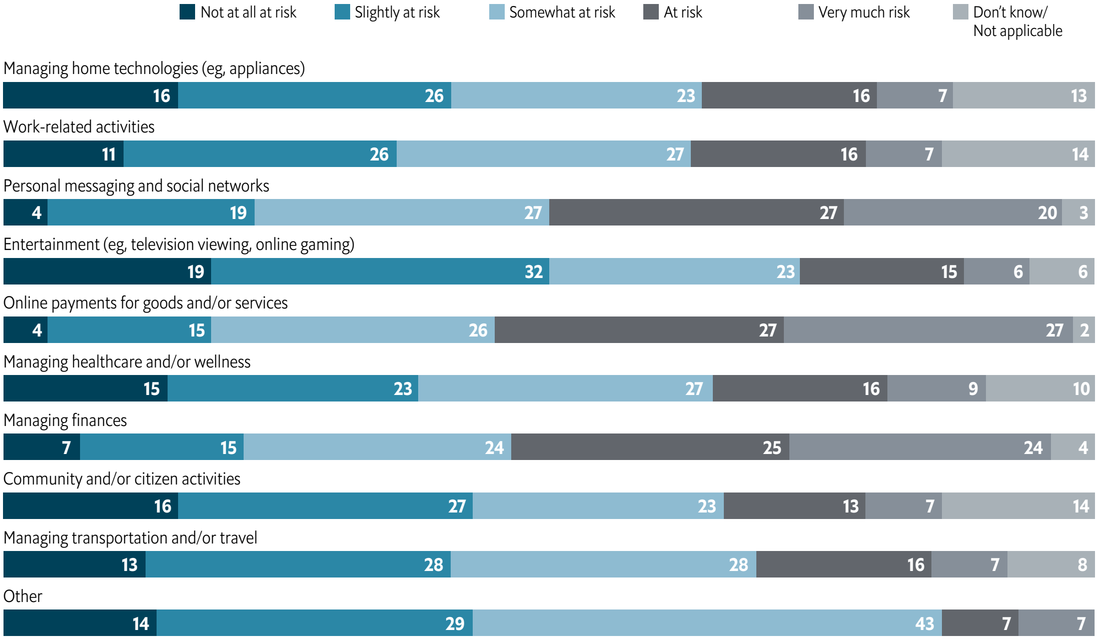
Please select all that apply.

(% of respondents)



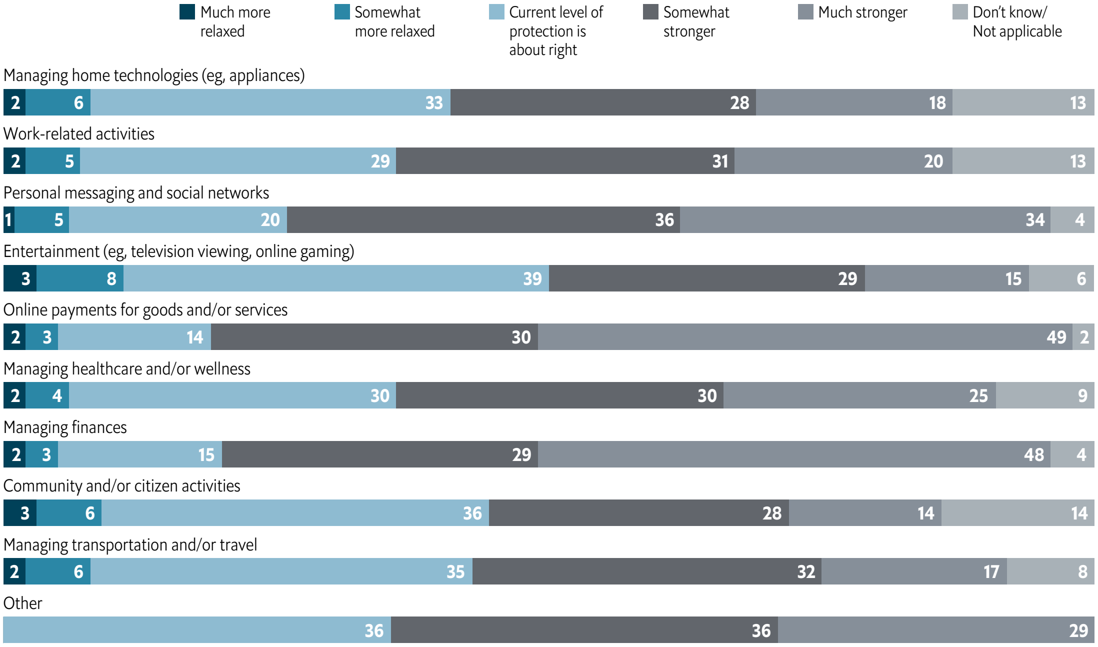
**To what extent do you believe that consumers put their personal privacy at risk in each of the following activities?**

(% of respondents)



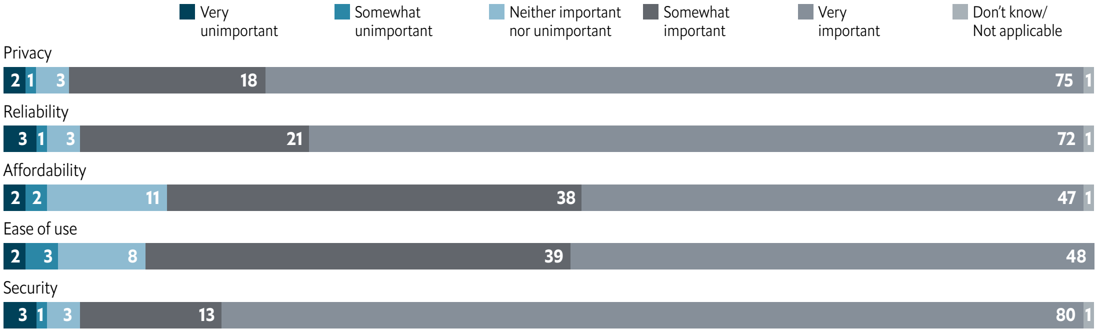
### How strong should consumer privacy protections be for each of the following activities?

(% of respondents)



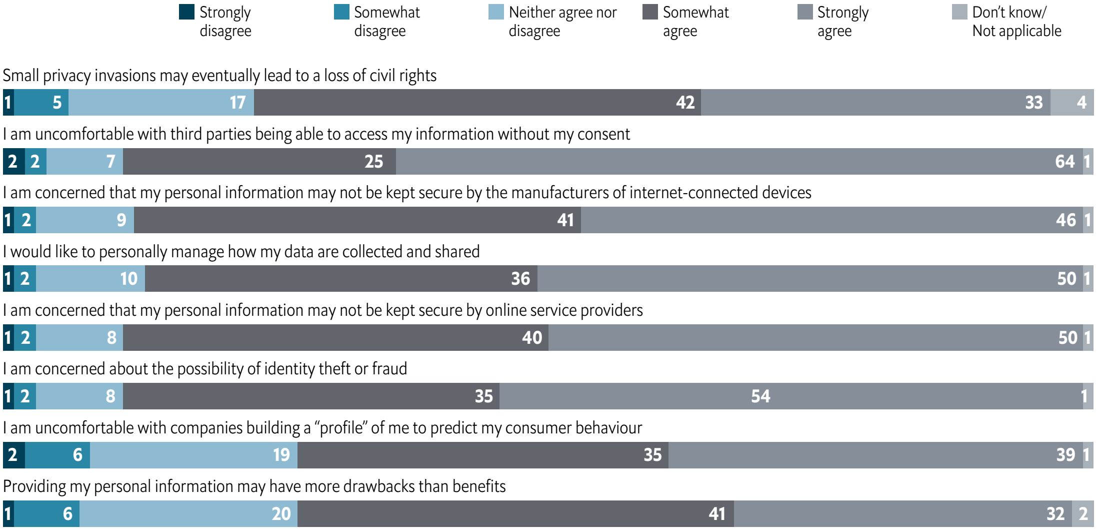
### Thinking about internet-connected devices in general, how important are each of the following issues to you?

(% of respondents)



**To what extent do you agree or disagree with the following statements?**

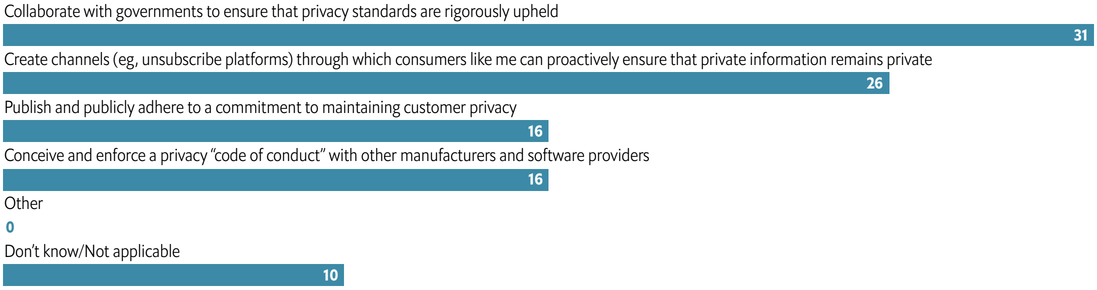
(% of respondents)



**Which of the following measures by device manufacturers and service providers would be most likely to make you more confident that your information is being kept private and secure?**

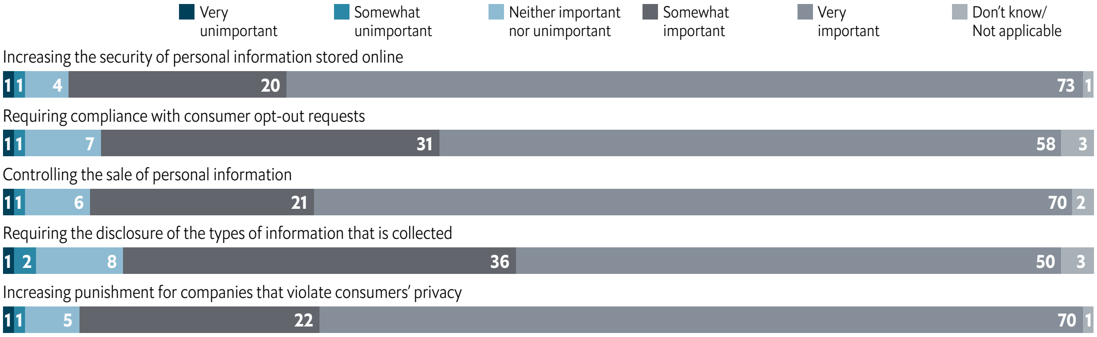
Please select one.

(% of respondents)



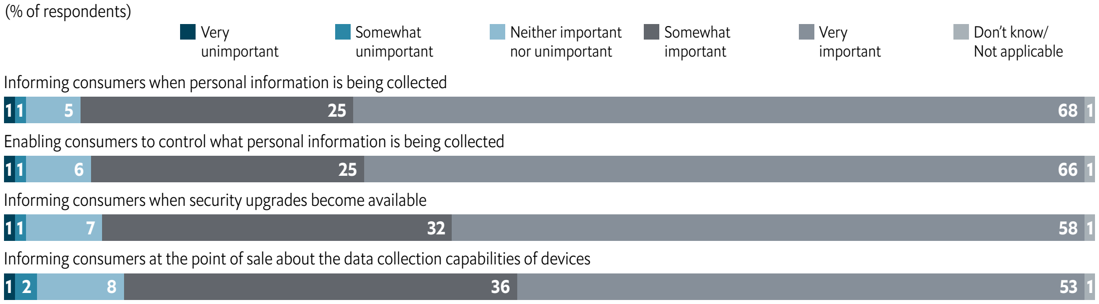
**How important are each of the following actions in terms of protecting the personal information consumers voluntarily provide online?**

(% of respondents)



**Personal information is increasingly collected automatically by connected devices (for example, smartphone tracking of user location and behaviour). With this in mind, how important are each of the following actions in terms of protecting the personal information consumers provide for automatic collection?**

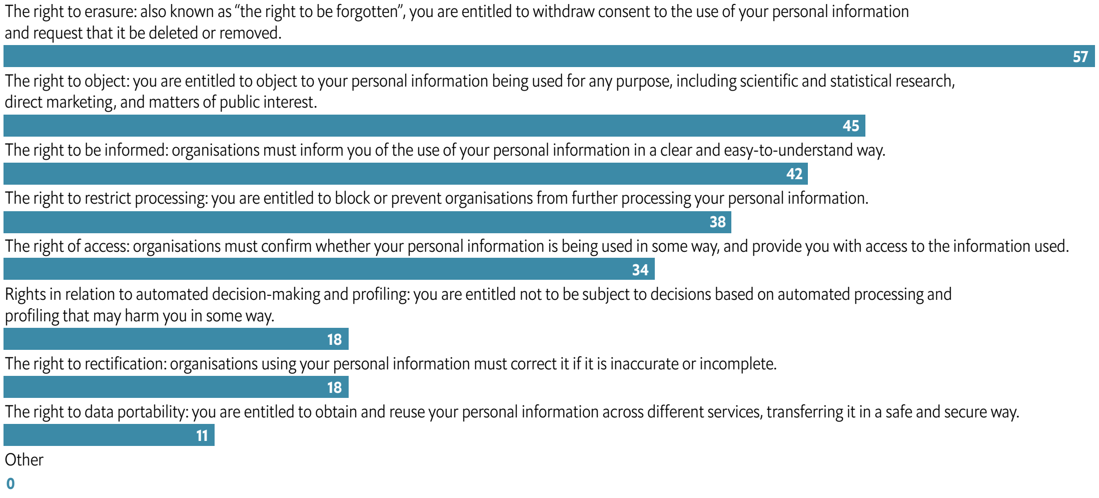
(% of respondents)



**Thinking about your personal information and how it might be used by third parties, which of the following rights do you consider most important?**

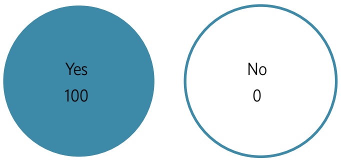
Please select up to three.

(% of respondents)



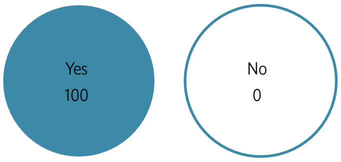
### Do you use internet-connected devices to make purchases, access business services or perform tasks that require you to reveal personal information (such as your name, date of birth or credit card number)?

(% of respondents)



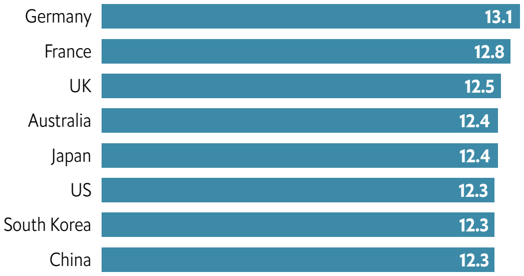
### Do you ever have thoughts or concerns about your online privacy and data security?

(% of respondents)



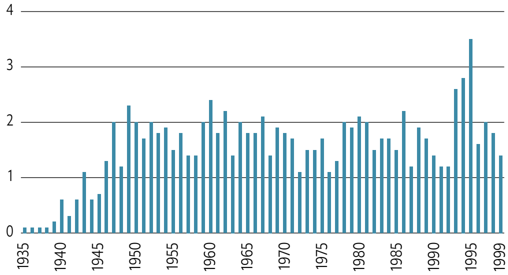
### In which country are you personally located?

(% of respondents)



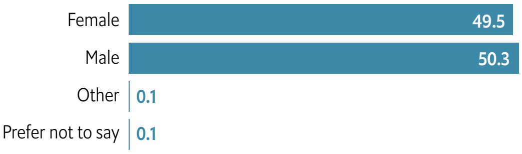
### Choose your year of birth

(% of respondents)



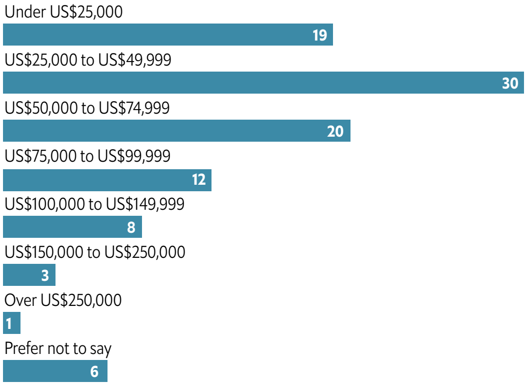
### With what gender do you identify?

(% of respondents)



### What is your approximate annual household income?

(% of respondents)



While every effort has been taken to verify the accuracy of this information, The Economist Intelligence Unit Ltd. cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report. The findings and views expressed in the report do not necessarily reflect the views of the sponsor.

**London**
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

**New York**
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 0248
E-mail: newyork@eiu.com

**Hong Kong**
1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

**Geneva**
Boulevard des
Tranchées 16
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com

**Dubai**
Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
E-mail: dubai@eiu.com