November 2018

The Internet Society Survey on Policy Issues in Asia-Pacific 2018

Focus: IoT Security and Privacy

Internet Society

Table of Contents

Executive Summary 3
Introduction 4
Key Findings 5
Conclusion 8

Disclaimer: The opinions, findings and conclusions in this report reflect the views of the survey respondents and not necessarily those of the Internet Society.

Executive Summary

An initiative of the Asia-Pacific Regional Bureau, the Internet Society Survey on Policy Issues in Asia-Pacific is an annual survey of the attitudes of Internet users towards topical Internet policy concerns. Now in its fifth instalment, this year's survey focuses on the security and privacy of the Internet of Things (IoT)—the rapidly expanding network of devices, physical objects, services and applications that communicate over the Internet. The IoT promises convenience, efficiency and insight, but it has also made vast quantity of data available. Moreover, many of today's IoT devices are rushed to market with little consideration for basic security and privacy protections, further heightening the risks that consumers face when using these devices. The survey, conducted from 1 June to 3 August 2018 and answered by 951 Internet users across 22 Asia-Pacific economies, examines how consumers in the region perceive and deal with IoT security and privacy risks. The survey also seeks to identify the top Internet-related policy concerns in the region.

Key Findings

Many Asia-Pacific consumers already own IoT devices and plan to purchase more.
Seven in ten respondents own at least one IoT device, and almost half of these respondents already own three or more IoT devices. Close to three-quarter of the respondents have plans to purchase an IoT device in the next 12 months.

Consumers want to own IoT devices, but they are also deeply concerned about their security and privacy.
Over half of the respondents lack confidence that IoT devices are sufficiently secure, and a similar percentage feel that they do not have enough information on the security of their device. Nine in ten respondents do not fully trust IoT manufacturers and service providers to secure their device.

Consumers' concerns about security and privacy do not match their ability to protect themselves.
Despite grave concerns about IoT security and privacy, many respondents have not taken any measures to protect themselves from IoT threats. Only half of those who own at least one IoT device have changed the default password on all their IoT devices, and only one in three have read the privacy policy that came with the device. Although there may be increasing awareness around the need for IoT security and privacy, efforts also need to be made to empower consumers with choices, tools and capabilities to take control of their security and privacy.

Asia-Pacific consumers want to be informed and have more control over their security and privacy. They highly value measures to protect against security and privacy threats, and believe that government should help ensure that these measures are in place.
Nine in ten respondents would like for security and privacy protections to come as a standard for all IoT devices, and a similar number indicate that they are likely to purchase IoT devices that have a security guarantee (through a trustmark or certification label). Moreover, over 70% of respondents would like to be given more control over the collection and use of their personal information. There is a need for policy, regulatory and technological interventions to ensure that manufacturers and suppliers of IoT products and services protect consumers and the privacy of their data. Three-quarter of the respondents believe that government plays a key role in this process.

Cybersecurity continues to be the top Internet policy concern in the Asia-Pacific region.
For two years in a row, cybersecurity has been the topmost concern in the Asia-Pacific region. Respondents have continued to find roughly the same issues significant over the last four years: access, data protection, connectivity and privacy, along with cybersecurity. Concerns about IoT and child online protection have become more prominent this year, while cloud computing and e-commerce have dropped in importance.

These findings have important implications on IoT adoption and stress the need to build customer trust in IoT products and services right from the start. We are at a critical juncture when we need to take vital steps to protect users and their data, and at the same time, empower users to take control of their security and privacy. A collaborative approach involving government, industry and civil society will be key to ensuring that IoT consumers are safe, innovation can flourish, and we can all fully benefit from IoT and its applications.

Introduction

An initiative of the Asia-Pacific Regional Bureau, the Internet Society Survey on Policy Issues in Asia-Pacific is an annual survey of the attitudes of Internet users towards topical Internet policy concerns. Now in its fifth instalment, this year's survey focuses on the security and privacy of the Internet of Things (IoT) devices—the rapidly expanding network of devices, physical objects, services and applications that communicate over the Internet (e.g., fitness tracker, smart TV, babycam).

The IoT promises convenience, efficiency and insight, but it has also made vast quantity of data available. At the same time, many of today's IoT devices are rushed to market with little consideration for basic security and privacy protections, further heightening the risks that consumers face when using these devices. The survey examines how consumers in the region perceive and deal with IoT security and privacy risks, as well as gauges their IoT security and privacy concerns and priorities.

This report provides an overview of the survey's findings, which are intended to contribute to policy debates and discussions—both in the region and globally.

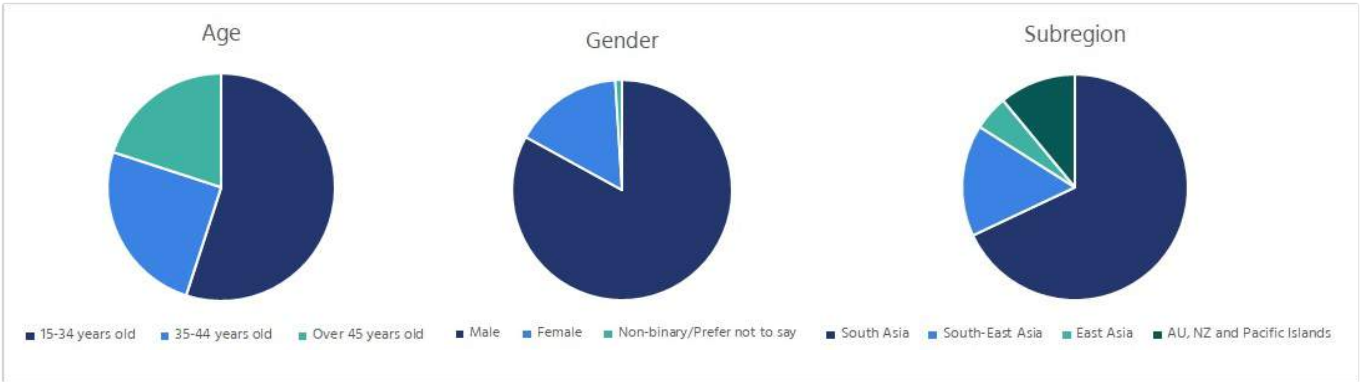
Background and Methodology

The survey was conducted online using the Survey Monkey platform, and ran from 1 June to 3 August 2018. The link to the questionnaire was disseminated via email to and through the 22 Internet Society Chapters, to Internet Society individual members in the Asia-Pacific region, to subscribers of the Asia-Pacific Regional Bureau's monthly newsletter—APAC Connections, and was publicised on social media platforms. It was open to the general public to gain as much input as possible.

The survey was administered in English and divided into three main sections. The first set of questions aimed to solicit views on IoT security and privacy risks, while the second section sought to identify the top Internet-related policy concerns in the region. The third section helped to determine the profile of the sample population.

Some 951 individuals from 22 economies across Asia-Pacific answered the survey. Sixty-eight percent of the respondents self-identified as residing in or originating from South Asia, with the rest coming from South-East Asia (16%); East Asia (5%); and Australia, New Zealand and the Pacific Islands (11%).The majority (91%) are members of the Internet Society, and are male (83%). Respondents are scattered across all age groups, but lean towards a younger demographic—55% are between 15-34 years old, 25% are aged 35-44, and the remaining 20% are 45 years or older. Respondents are quite evenly distributed across organizational affiliation—24% are with the technical community, 23% with academia, 20% with civil society, 19% with the private sector and 14% with government. The majority (93%) are familiar with IoT, with almost two-third of the respondents believing that they fully understand what IoT is.

Figure 1. Summary of respondents' profile

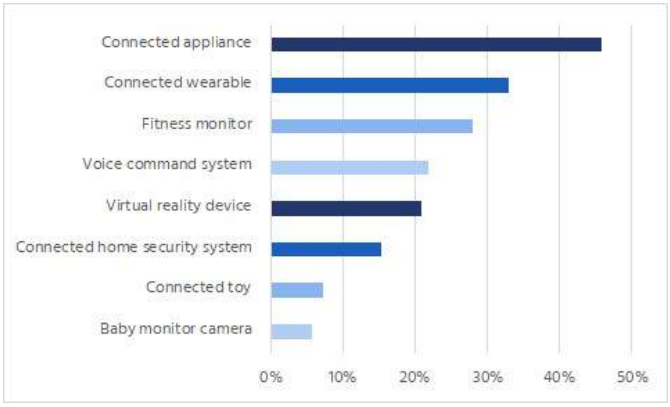


It should therefore be noted that the results of this survey are more weighted towards perspectives from South Asia, and a young, tech-savvy male population. Nevertheless, this report has looked at, and presents both the overall and disaggregated findings based on gender and subregion.

Key Findings

Many Asia-Pacific consumers already own IoT devices and plan to purchase more.

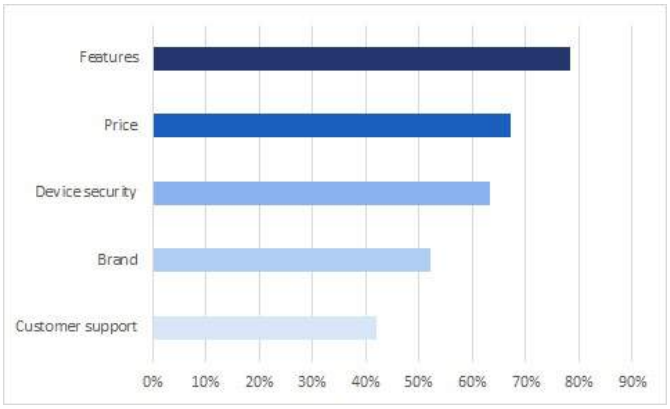
Figure 2. Types of IoT devices that respondents own



Seven in ten respondents own at least one IoT device, and almost half of these respondents already own three or more IoT devices. The most common IoT devices owned by respondents include connected appliances (e.g., smart TV, smart fridge), connected wearables (e.g., smart watch), fitness monitors, voice command systems (e.g., Google Home, Amazon Alexa), and virtual reality devices (e.g., headsets) (see Figure 2). Men tend to own more IoT devices than women, and more women (40%) than men (30%) do not own any IoT device. Close to three-quarter of the respondents plan to purchase an IoT device in the next 12 months.

Consumers want to own IoT devices, but they are also deeply concerned about their security and privacy.

Figure 3. Factors influencing consumers' decision to purchase IoT devices



For the majority of the respondents, the smart features and price of the IoT devices are driving purchases and ownership, but two in three respondents believe security is one of the factors that will influence their purchasing decision (see Figure 3).

Over half of the respondents lack confidence that IoT devices are sufficiently secure, and a similar percentage feel that they do not have enough information on the security of their device. Nine in ten respondents do not fully trust IoT manufacturers and service providers to secure their device. And 60% of the respondents who do not own an IoT device believe that they are unlikely or highly unlikely to use an IoT device if there are no guarantees that the personal information captured will be fully protected. Furthermore, the majority of the respondents express concern about the following:

- 81% are concerned about their personal information being leaked
- 73% are concerned about hackers taking control of their device and using it to commit crime
- 72% are concerned about hackers gaining access to personal information
- 71% are concerned about being monitored without their knowledge or consent

Consumers' concerns about security and privacy do not match their ability to protect themselves.

Despite grave concerns about IoT security and privacy, many respondents have not taken any measures to protect themselves from IoT threats. Only half of those who own at least one IoT device have changed the default password on all their IoT devices, and only one in three have read the privacy policy that came with the device. Among those who have not changed the default password on their device, 30% made the decision not to use a password and about 10% did not know how to change it. Approximately half of the respondents claim that their devices do not have a password, but it could also be possible that they were not aware that their devices had one.

Although there may be increasing awareness around the need for IoT security and privacy, efforts also need to be made to empower consumers with choices, tools and capabilities to take control of their security and privacy. These include providing clear instructions on how to change the default password and adjust security and privacy settings, as well as presenting easily understandable privacy notices and choices to customers in the set up or purchase of an IoT device.

Asia-Pacific consumers want to be informed and have more control over their security and privacy. They highly value measures to protect against security and privacy threats, and believe that government should help ensure that these measures are in place.

Hand-in-hand with raising consumers' awareness and capabilities, there is a need for policy, regulatory and technological interventions that ensure manufacturers and suppliers of IoT products and services protect consumers and the privacy of their data. Survey respondents highly value some of the potential measures to safeguard their security and privacy. For instance, nine in ten respondents would like for security and privacy protections to come as a standard for all IoT devices, and a similar number indicate that they are likely to purchase IoT devices that have a security guarantee (through a trustmark or certification label).

Giving consumers more control over the collection and use of their personal information appears to be an essential aspect of ensuring trust in IoT products and services. Most respondents would like to have the following options/information available to them:

- The option to delete personal data collected (84% of respondents)
- Know what kinds of personal data the IoT device captures (84%)
- Know who can access this information (83%)
- Know how this information is used (77%)
- Know where this information is stored (72%)

Government plays a key role in promoting security and privacy in IoT products and services. Three-quarter of the respondents feel that government should intervene to ensure the security of IoT devices.

Cybersecurity continues to be the top Internet policy concern in the Asia-Pacific region.

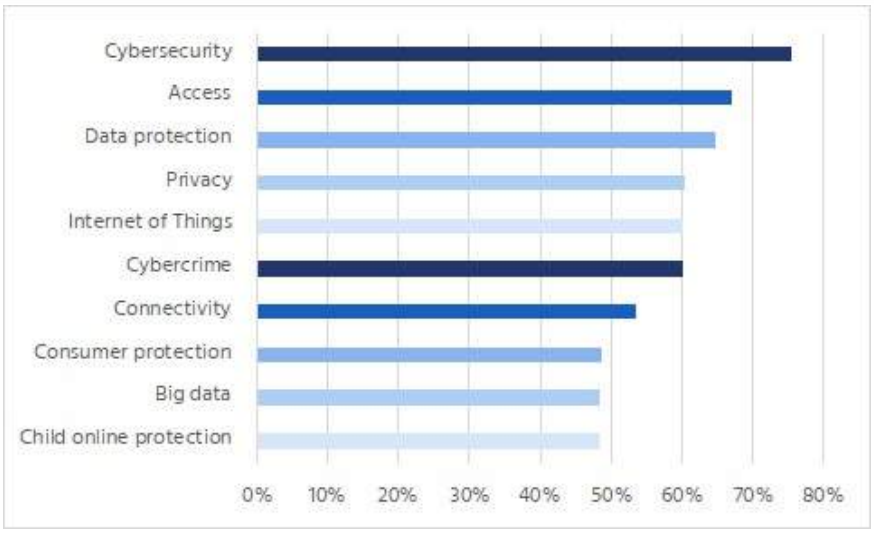
Figure 4. Top five policy concerns from 2014 to 2018

Policy Issue	2014	2015	2016	2017	2018
Access	✓	✓	✓	✓	✓
Connectivity	✓	✓	✓	✓	
Data protection	✓	✓	✓	✓	✓
Cybersecurity	✓		✓	✓	✓
Privacy			✓	✓	✓
Cloud computing	✓	✓			
E-commerce		✓			
Internet of Things					✓

For two years in a row, cybersecurity has been the topmost concern in the Asia-Pacific region. Over the past year, Internet users across Asia-Pacific have been monitoring cybersecurity, access, data protection, privacy and IoT issues, above other policy-related concerns in the region. These have remained more or less constant since 2014 (see Figure 4). IoT has risen from its usual top ten position to the top five. However, it is possible that this may be because the focus of this year's survey is IoT-related.

Cloud computing and e-commerce have dropped from Internet users' radar to be replaced by concerns related to child online protection. Other issues that have remained a priority for a number of years now include connectivity, big data, consumer protection and cybercrime (see Figure 5).

Figure 5. Top ten policy concerns in 2018



In Pacific Island countries,[1] users are most concerned about access, connectivity and cybersecurity. Moreover, they pay more attention to policies related to the Internet (digital) economy and over-the-top services (e.g., Whatsapp, Skype), over big data and consumer protection, when compared with the regionwide average in Figure 5.

Indian nationals, which make up a quarter of the survey respondents, are more concerned about net neutrality than others.

In high-income economies,[2] issues related to freedom of expression, censorship, content filtering, encryption, and government and commercial surveillance are top of mind, instead of connectivity, child online protection, cybercrime and IoT (when compared with regionwide user priorities).

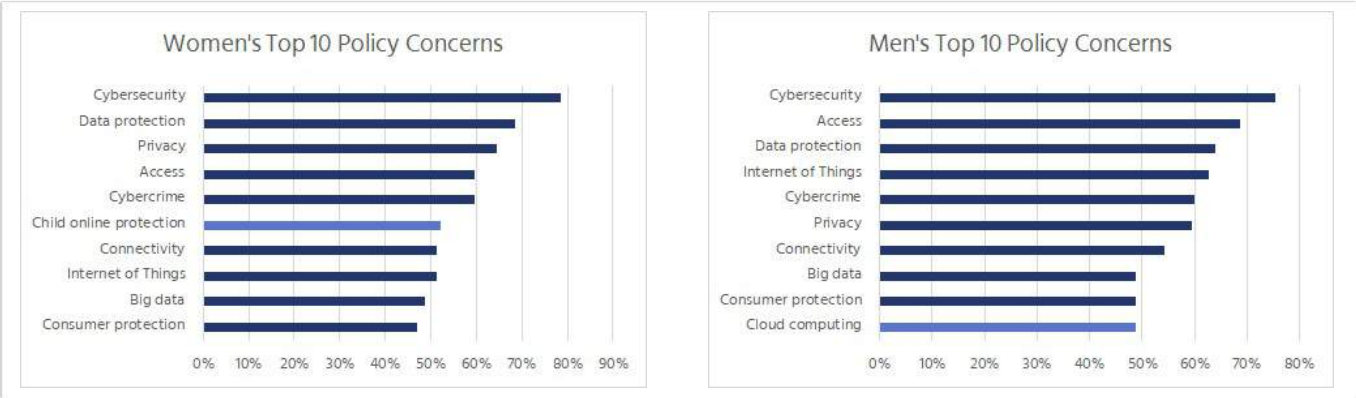
[1] There were 45 respondents from the following Pacific Island countries: Papua New Guinea (50%), Fiji (25%), Kiribati, Marshall Islands, Nauru, New Caledonia, Palau, Samoa, Tonga and Vanuatu.

[2] The high-income economies include Australia, Hong Kong, Japan, Republic of Korea, Macao, New Zealand, Singapore and Taiwan, with 80 respondents.

Generally, women and men have similar policy concerns.

The top-ten policy concerns for both the female and male respondents are very similar. The only exception is women prioritizing child online protection, while men seem to pay more attention to issues around cloud computing (see Figure 6).

Figure 6. Top ten policy concerns of female and male respondents



Conclusion

The survey yields several findings that are significant to the development of IoT security and privacy in the region. Firstly, consumers are owning an increasing number of IoT devices, but are concerned about security and privacy threats. Secondly, many are aware that their devices are not sufficiently secure and their information not fully protected. More importantly, most do not fully trust IoT manufacturers and service providers to secure their devices. Although consumers claim that device security is not the number-one factor influencing their purchasing decision, many remain hesitant to use IoT products and services that do not have security and privacy guarantees. These have important implications on IoT adoption, and stress the need for IoT manufacturers and suppliers to build customer trust in IoT products and services right from the start.

Consumers want to be informed, and have a greater level of control over the collection and use of their personal information. However, to date, consumers are struggling with the lack of tools and resources available for them to exercise their security and privacy rights. Interventions such as security and privacy standards for IoT devices, security guarantees through a trustmark or certification label, and the option to delete personal data collected, are all highly favoured by most respondents.

Overall, respondents have continued to find roughly the same issues significant over the last four years: access, data protection, connectivity and privacy, with cybersecurity keeping the top spot this year. Concerns about IoT and child online protection have become more prominent, while cloud computing and e-commerce have dropped in importance.

IoT is poised to transform economies and societies worldwide. The technology brings enormous opportunities, but also significant security and privacy risks. We are at a critical juncture when we need to take vital steps to protect users and their data, and at the same time, empower users to take control of their security and privacy. A collaborative approach involving government, industry and civil society will be key to ensuring that IoT consumers are safe, innovation can flourish, and we can all fully benefit from IoT and its applications.

Please send comments and feedback to:

Internet Society - Asia-Pacific Bureau
9 Temasek Boulevard
#09-01 Suntec Tower 2
Singapore 039898

Tel – +65 6407 1470
Fax – +65 6407 1501
E-mail – apac@isoc.org

Facebook – /isocasiapacific/
Twitter – @ISOCapac
Scoop.it! – http://www.scoop.it/t/internet-in-asia-pacific
Subscribe to newsletter – http://bit.ly/ISOC-APAC-signup