Mobile and Privacy

MOBILE PRIVACY:

Consumer research insights and considerations for policymakers

February 2014

MOBILE INTERNET: MAXIMISING GLOBAL OPPORTUNITIES AND ADDRESSING PRIVACY CHALLENGES

The mobile industry has scaled dramatically over the last decade. At the end of 2003, there were over one billion unique subscribers, with this figure increasing to

3.4 BILLION

by the end of 2013. The number of mobile broadband connections also grew tenfold from just over 200 million in 2008, to more than **two billion by 2013.**

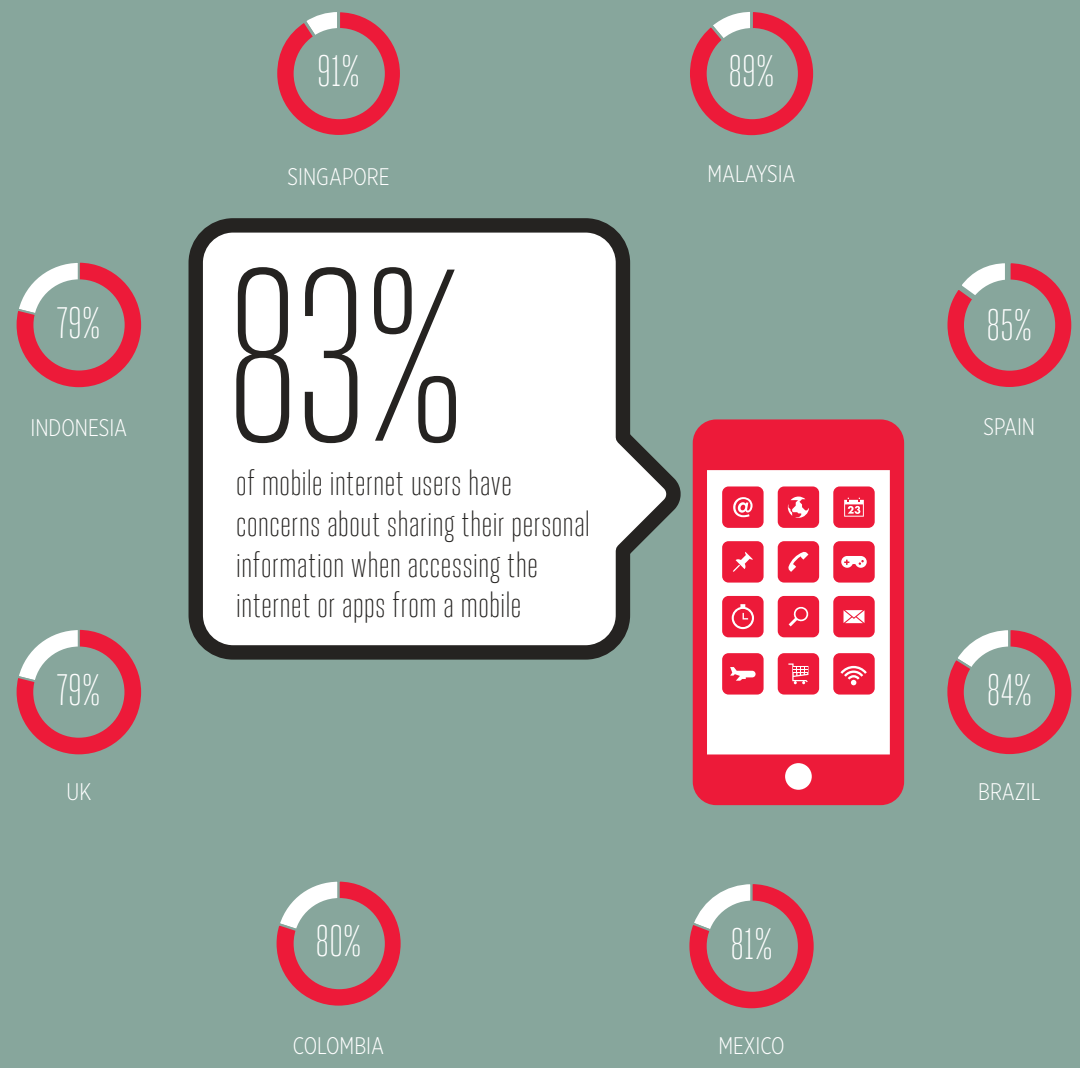
The growth in mobile broadband connections has been fuelled by higher speed networks and more advanced technologies. Additionally, the proliferation of new apps and services are allowing people to connect with each other, devices and other 'smart' objects (such as cars, home utility meters and health monitoring devices) in exciting new ways. Although the ability to connect with apps and services is bringing huge benefits to consumers and societies, it is also creating a number of privacy challenges and giving rise to concerns as consumer data is increasingly accessed, used and shared by multiple parties.

The GSMA has been working closely with its members to proactively address key mobile privacy challenges and, as part of this, commissioned global research on more than **11,500 mobile users (Brazil, Colombia, Indonesia, Malaysia, Singapore, Spain and the UK).** The research examines users' privacy concerns and how they influence attitudes towards the mobile internet and apps, and the adoption of these services. The findings show that mobile users from all countries share similar attitudes and concerns about their privacy. This paper presents the key research findings and discusses the implications for policymakers.

MOBILE USERS' PRIVACY FEARS ARE HOLDING BACK THE GROWTH OF MOBILE APPS AND SERVICES

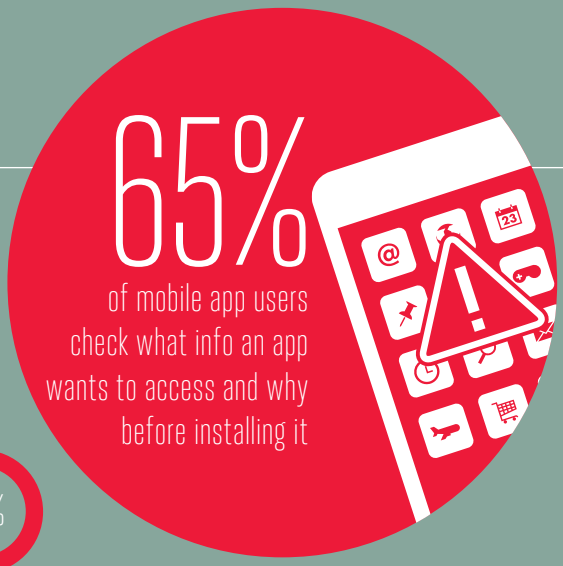
Over **80 per cent** of mobile internet users worldwide were concerned about sharing their personal information when accessing apps and services (Figure 1). Further, before installing an app, the majority of app users seek to find out what information it wants to access on their device, demonstrating a desire to understand how their privacy might be affected (Figure 2). Most mobile users also want to be asked for permission before 3rd parties access their personal information on their mobile devices, and to have more control over the types of data different companies might access (Figure 3). Importantly, almost half of app users would limit their use of apps unless they were sure their personal information was safe (Figure 4).

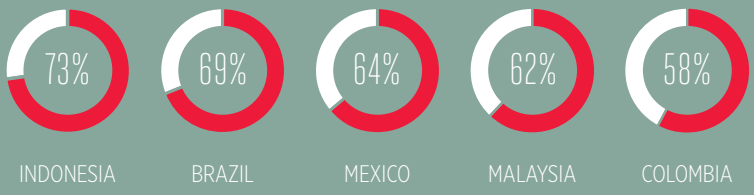
Figure 1:
Levels of concern about sharing personal information when using mobile internet and apps



Base: All mobile internet users

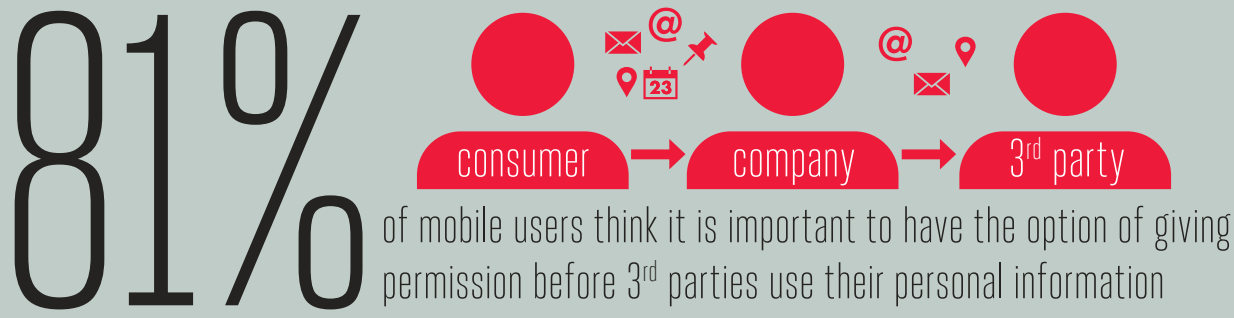
Figure 2:
The extent to which mobile app users seek to understand what personal information an app wants to access

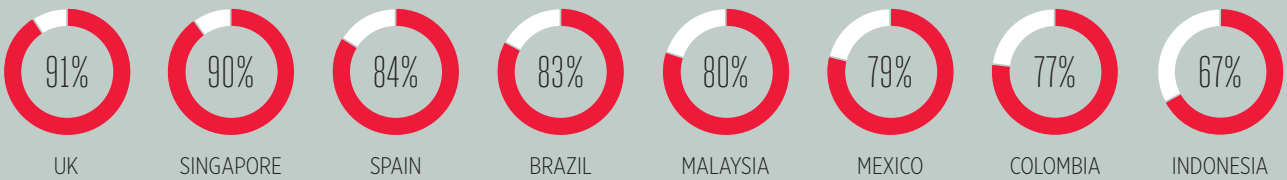




Base: All mobile app users (comparable data not available for UK, Spain and Singapore)

Figure 3:
Attitudes towards 3rd parties accessing mobile users' personal information



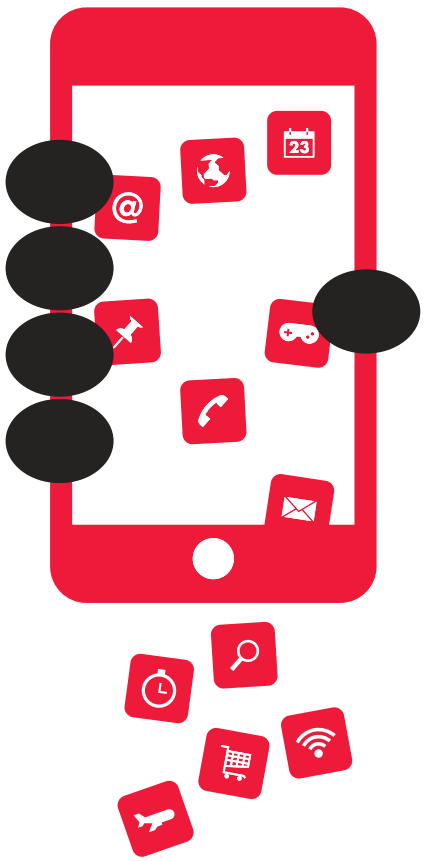


Base: All mobile internet users

The research showed that over 90 per cent of mobile users in the UK and Singapore want to be asked for their permission before 3rd parties use their personal information, and many users in other countries share these opinions (Figure 3). Indonesian mobile app users appear to be the least concerned (although the results are still high at 67 per cent), but are most likely to limit their use of apps unless they were sure their information was safe (Figure 4).

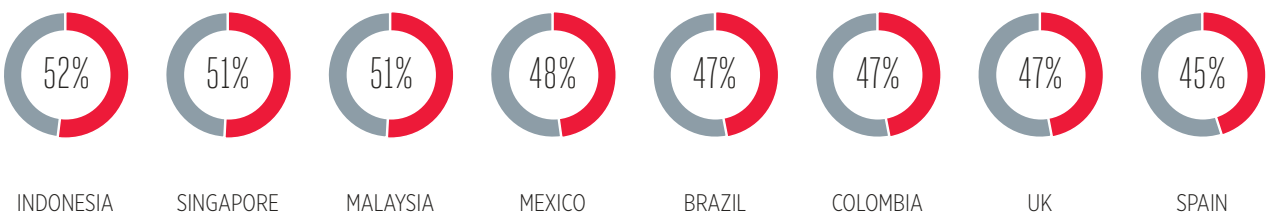
Maintaining mobile users' confidence and trust is crucial when developing new mobile services such as Mobile Commerce[1], Mobile Identity[2] and Mobile Government[3]. User trust is also fundamental for maintaining the mobile industry's substantial contribution to the global and local economies; it is estimated that mobile operators alone contributed 1.4 per cent to global gross domestic product (GDP) in 2012[4]. Consequently, there is a strong incentive for both industry and policymakers to ensure mobile services respect users' privacy. For example, policymakers should take into account the fast-paced nature of technological developments and allow some flexibility in how privacy regulations are implemented. This would enable service providers to offer consumers simple and relevant mechanisms to manage their privacy preferences.

Figure 4:
The impact of privacy concerns on the use of apps



48%

of mobile app users with privacy concerns would limit their use of apps unless they felt sure their personal information was better safeguarded



Base: All Audience 'B' mobile app users

[1] http://www.gsma.com/mobilecommerce/ [2] http://www.gsma.com/mobileidentity/ [3] For example, see 'Mobile for Development' case studies at http://www.gsma.com/mobilefordevelopment/
[4] Source: A.T. Kearney – GSMA Mobile Economy report 2013. See http://www.gsmamobileeconomy.com/read/

MOBILE USERS WANT THEIR PRIVACY TO BE TREATED CONSISTENTLY

Online data protection and privacy are currently regulated by a patchwork of over 100 national and local laws — where they exist. However, mobile operators also abide by telecoms-specific rules and regulations, which internet and service providers are not subject to, even though they provide equivalent services and may collect and use similar or functionally equivalent data. For example, mobile operators have tight restrictions on the use of their customers' cellular location, whereas internet companies offering services that use the same customers' GPS or Wi-Fi location data have no such restrictions. Country- and technology-specific privacy laws are therefore increasingly unable to address emerging privacy risks and challenges associated with the global flows and contexts of users' mobile-derived personal information.

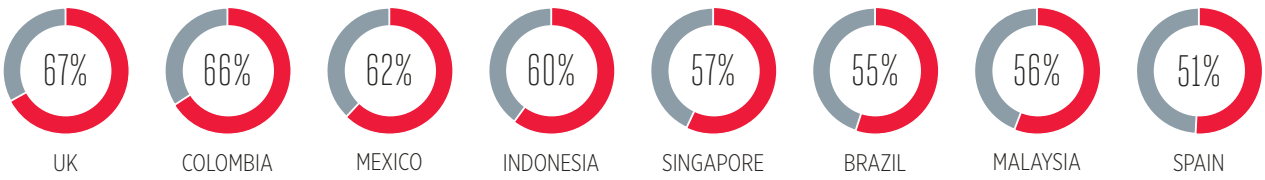
According to the research, six out of 10 mobile users want their privacy to be treated consistently, regardless of the device, business model and data flows involved, or the location of the companies accessing and collecting their data (Figure 5). Mobile users' privacy expectations are therefore not being met where companies dealing with their personal data are subject to different and inconsistent rules.

Many governments are currently introducing or updating their data protection and privacy laws and the GSMA welcomes policymakers' increased level of engagement with the wider industry in addressing mobile users' privacy concerns and needs.

Figure 5:
The importance of having consistent rules applicable to companies accessing mobile users' location data

60%

of mobile users want a consistent set of rules to apply to any company accessing their location, regardless of how they obtain this information



Base: All Audience 'A' mobile users

CONSIDERATIONS FOR POLICYMAKERS

WHEN CONSIDERING REGULATORY APPROACHES TO MOBILE USERS' PRIVACY, IT IS IMPORTANT THAT POLICYMAKERS:

- Engage with the wider mobile industry to understand the implications of technological developments on users' privacy
- Identify and address privacy challenges in ways that are technology-neutral and that reflect the global nature of services and data flows
- Understand mobile users' concerns and the contexts in which these are raised
- Learn from, share and develop best practices that support flexibility and innovation in the use of mobile-derived data, for example by promoting the principle of "Privacy by Design"

MOBILE USERS WANT TO MANAGE THEIR PRIVACY IN CLEAR, SIMPLE AND UNOBTRUSIVE WAYS

Many online services, including apps require users' permission (often at the point of installation) to enable the service to access data on their device. While some of that data may be necessary for the service or app to operate, other types of data may be used (by the app, software or hardware developer) for commercial purposes, particularly in cases where apps or services are offered for free. For example, developers often build databases of user-profiles (age, gender, location, preferences, contacts etc.) which may be sold to advertising companies to provide users with targeted ads.

The extent to which those user profiles are based on personal or identifiable information can have a direct impact on their privacy. It is therefore important that users are able to understand and control what personal information a mobile app or service can access and how this data might be used for advertising or other purposes. The research shows that 82 per cent of mobile users want to know when, and what type of, personal information is being collected from their mobile devices (Figure 6).

Currently, laws on whether user permission is required and how it should be obtained before a service can access their personal information differ between countries. Some online services display lengthy terms and conditions which the user has to agree to before using the app or service. However, the research shows that

8 OUT OF 10 USERS

AGREE TO PRIVACY NOTICES WITHOUT READING THEM BECAUSE THEY TEND TO BE TOO LONG OR LEGALISTIC (FIGURE 7)

Consequently, if mobile users are bombarded with privacy notices or requests to 'consent' to the use of their data, they are more likely to experience 'privacy notice fatigue' and simply click 'I agree' without reading the notice or understanding the implications of their decision.

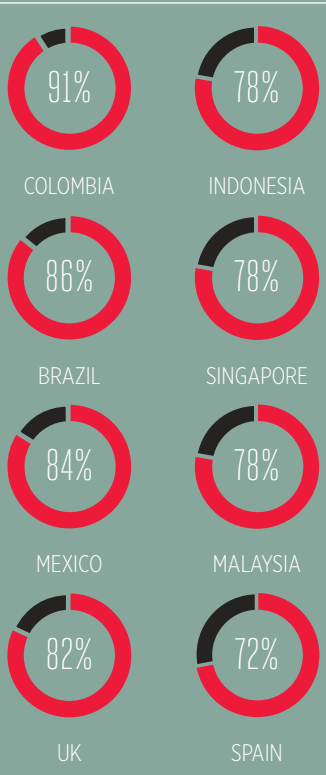
To avoid these issues, there is a need for more user friendly, contextual and nuanced approaches to providing transparency for users and helping them make informed choices about the use of their data. The research shows that 70 per cent of mobile users want to choose the type and frequency of ads they receive on their devices (Figure 8) while 75 per cent of mobile users think that a privacy icon might encourage them to accept targeted ads (Figure 9).

Although country differences in attitudes are not large, Latin American mobile users have the highest desire to understand what personal information companies collect from their devices, including 91 per cent of Colombian users (Figure 6). Latin Americans also have the highest desire to choose the types and timing of ads they receive on their devices (Figure 8).

Figure 6:
Mobile users' desire to understand what personal information is collected from their devices

82%

of all mobile users want to know when, and what type of personal information is being collected from their mobile devices



Base: All mobile users

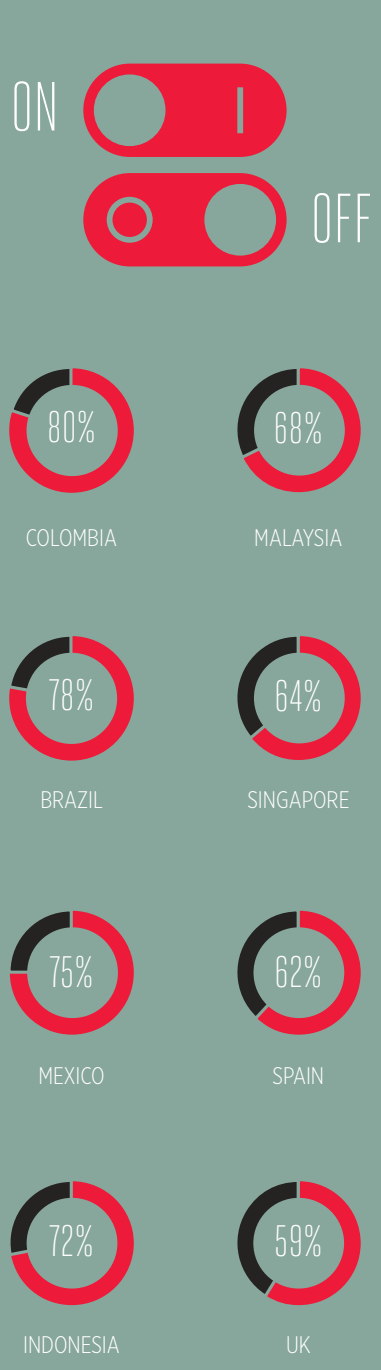
Figure 7:
Users choosing 'too long' as the key reason for agreeing to privacy notices without reading them

80%

of mobile internet users who "agree" to privacy policies without reading them said it is because they are "too long"

Base: All mobile internet users who always/often/sometimes "agree" to privacy statements without reading them (comparable data unavailable for UK, Spain and Singapore)

Figure 8:
Mobile users' desire to choose the types and timing of ads they receive on their devices



Base: All mobile users

Figure 9:
The potential impact of a privacy icon on mobile users' willingness to accept targeted ads

75%

of mobile users think that a privacy icon might encourage them to accept targeted ads

Base: All Audience 'A' mobile users

CONSIDERATIONS FOR POLICYMAKERS

WHEN CONSIDERING NEW REGULATORY APPROACHES TO MOBILE USERS' PRIVACY, IT IS IMPORTANT THAT POLICYMAKERS:

- Assess the potential impact of a policy on the user experience. For example, will the law encourage mobile users to make the right privacy decisions or will it over-burden them and generate 'privacy fatigue'?
- Take into account the small screen size of many mobile devices, by incentivising the development of simple display mechanisms that help users understand their privacy choices and manage how their data is used and shared. Examples may include:
    1. Icons or graphics indicating the type of information that an app wants to access
    2. Just-in-time messages reminding users of their privacy choices
- Avoid being too prescriptive in how service providers enable users to express choice and control over their privacy. Developers of mobile services and apps are best placed to:
    1. Understand any privacy risks posed by their specific service or app
    2. Offer users options to manage their privacy preferences depending on the context of each service and without frustrating their experience when using that service
- Conduct impact assessments before any proposed measures are agreed, for example by:
    1. Testing privacy management tools/icons on users to assess their effectiveness
    2. Examining the implications of new measures on business and innovation
    3. Considering their applicability across different platforms, devices and services

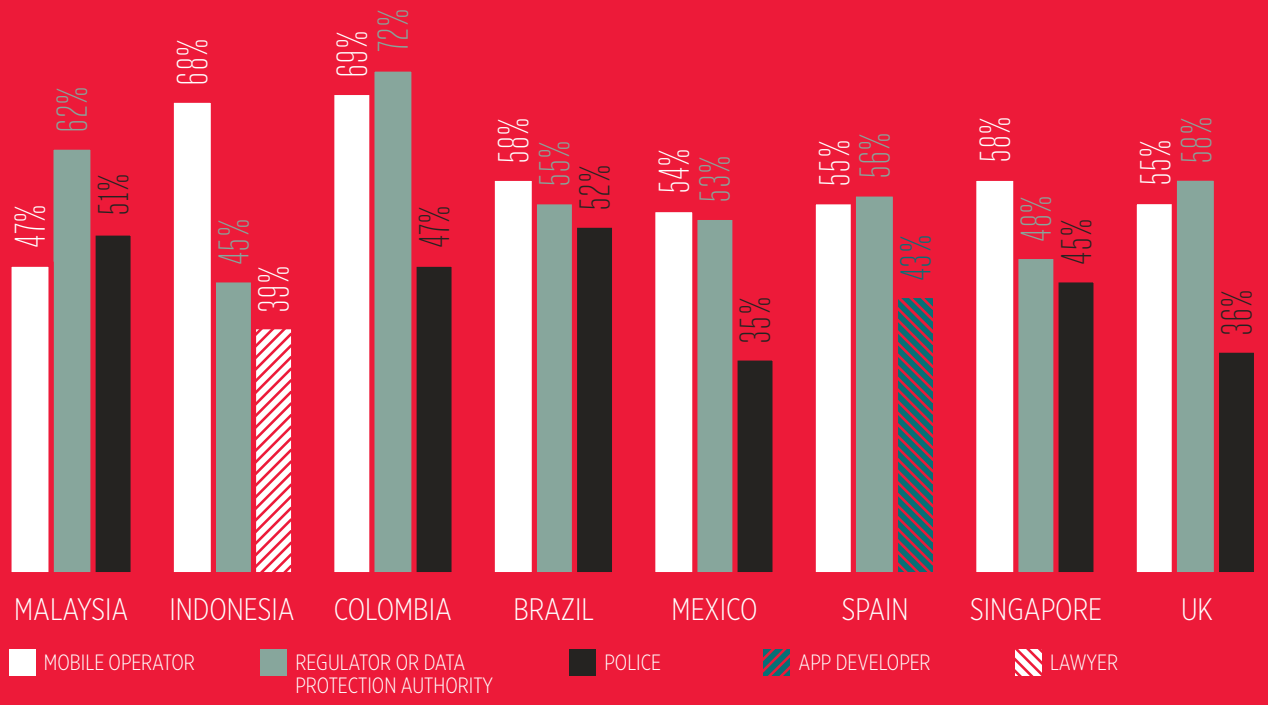
MOBILE USERS LOOK TO THEIR MOBILE OPERATORS TO SAFEGUARD THEIR PRIVACY

Since the early days of mobile telephony, operators have built trusted relationships with their customers, offering them valuable services while safeguarding their personal information.

However, the mobile internet has enabled users to build new relationships and share increasing amounts of personal information with a range of global service providers, which is beyond mobile operators' control. The GSMA's research shows that most users trust their mobile operators to safeguard their personal information and would contact them first if their privacy were breached (Figure 10). Moreover, most users hold their mobile operators responsible for safeguarding their personal information even in situations where the operators have no actual control over the data (e.g. personal information accessed by an app that a user downloads from an independent app store on their smartphone) (Figure 11).

Figure 10:
Who would mobile users turn to if they suffered a serious invasion of privacy whilst using a mobile app (top 3 choices, by country)

Globally, mobile users primarily look to their mobile operators (58%) for help when their privacy is invaded, followed by their national regulator/data protection authority (57%)

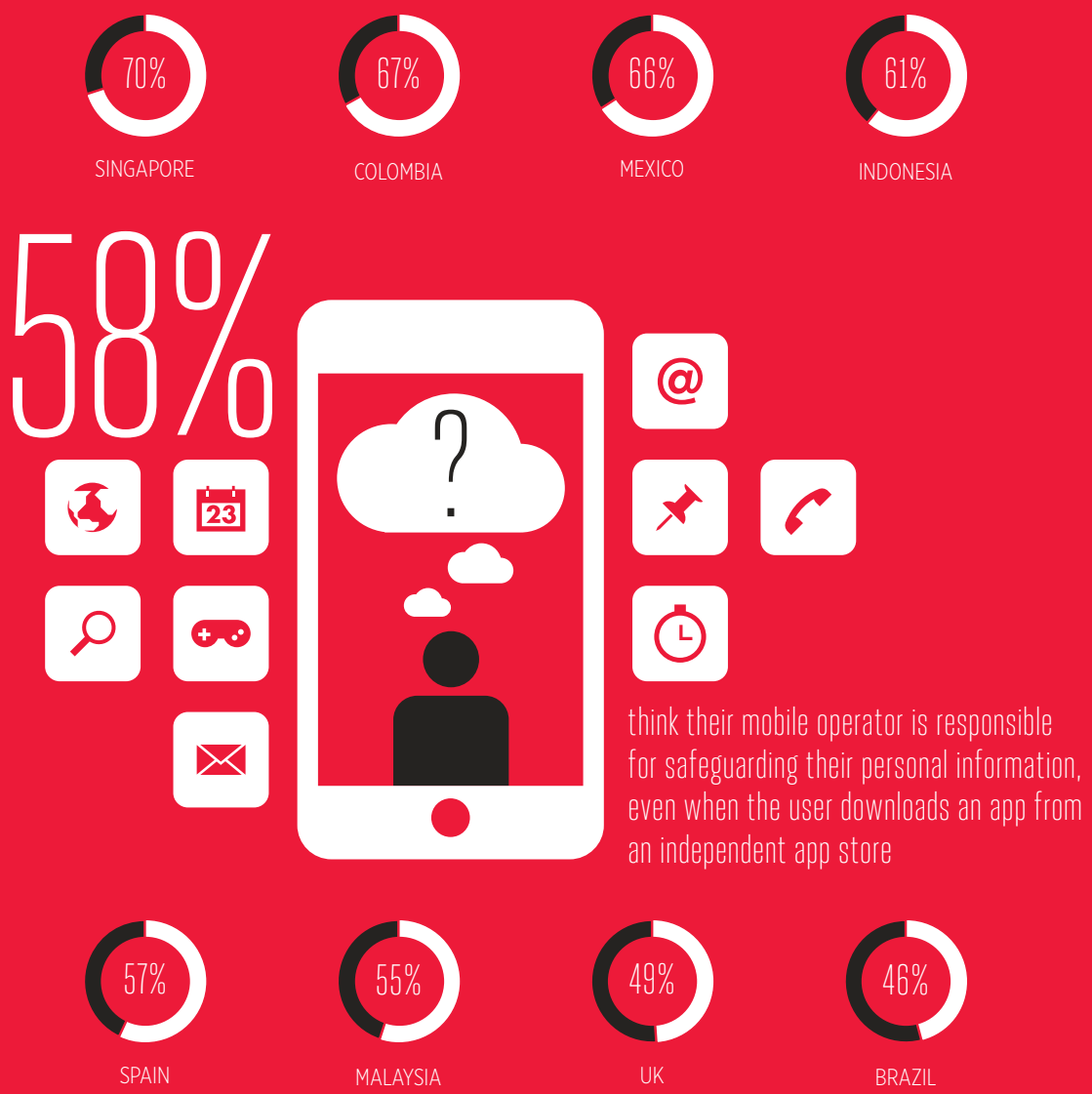


Base: All mobile users

Figure 10 shows that mobile users in seven out of the eight countries would look to their operator or regulator/data protection authority for help if their privacy were breached while using a mobile app. Malaysia appears to be the only exception, where mobile operators ranked third after regulator/data protection authorities and the police.

Furthermore, Figure 11 below suggests that mobile users in Colombia, Indonesia, Mexico and Singapore are relatively less aware of their mobile operators' inability to safeguard their privacy in scenarios where the user interacts with 3rd parties, for example when they download an independent mobile app. In such situations, it is the 3rd party (app developer or app store) that controls what information the app can access and not the mobile operator. Education and transparency are therefore necessary to ensure users understand the respective responsibilities and roles of different parties in safeguarding their personal information.

Figure 11:
Mobile users' perceptions of the mobile operators' responsibility to safeguard their privacy (even when the mobile operator has no actual control)



Base: All mobile users

CONSIDERATIONS FOR POLICYMAKERS

BEFORE INTRODUCING OR UPDATING ONLINE PRIVACY LAWS, POLICYMAKERS MAY CONSIDER:

- Distinguishing the different types of companies involved in the provision of online services, and understanding their respective roles and responsibilities in safeguarding mobile users' privacy

- Promoting industry-wide and technology-neutral codes or guidelines* that apply to all companies dealing with consumers' personal information. These could highlight:
    1. Examples of responsible and accountable business practices
    2. Ways to mitigate foreseeable risks e.g. the possibility of a privacy breach
    3. Possible mechanisms to help users manage their privacy preferences
    4. Effective redress mechanisms in case of a privacy breach

- Developing or incentivising 'mobile education' campaigns to help users understand:
    1. How the mobile internet works and how information is captured and used, (including the legitimate uses of data)
    2. What different technologies and services aim to achieve - removing unnecessary consumer fear and anxiety
    3. The implications of sharing personal information with different companies
    4. The responsibilities of different companies across the mobile ecosystem in safeguarding the personal information of users

* For example, the GSMA's Privacy Design Guidelines for Mobile Application Development
http://www.gsma.com/publicpolicy/mobile-and-privacy/design-guidelines

RESEARCH METHODOLOGY AND SAMPLE OVERVIEW

The research was conducted by Futuresight Ltd, an independent research agency, on behalf of the GSMA, and covered eight countries. The research in each country involved two parts:

(a) An online quantitative survey covering more than 11,500 respondents across the eight countries; and

(b) Small-scale face to face interviews with mobile internet and app users in each country to add qualitative diagnostics to the quantitative results.

The sample was broadly representative in terms of demographics (age, gender, social grade and region), albeit older age groups were slightly under-represented, as is common with online panels. Similarly, the sample was also representative of the mobile industry supply side in each country, i.e. in terms of handset manufacturer brands, payment models (prepaid and post-paid) and mobile network operators. In terms of usage, the sample was overall more biased towards smartphone/ sophisticated users of the mobile internet and apps

COUNTRY	TOTAL SAMPLE	SMARTPHONE USERS	RESEARCH CONDUCTED IN
MALAYSIA	1,504	87%	JULY 2013
INDONESIA	1,527	87%	JULY 2013
COLOMBIA	1,511	67%	MARCH 2013
BRAZIL	1,505	64%	NOVEMBER 2012
MEXICO	1,503	76%	NOVEMBER 2012
SPAIN	1,094	65%	APRIL – JUNE 2011
SINGAPORE	1,005	87%	APRIL – JUNE 2011
UK	2,022	50%	APRIL – JUNE 2011
OVERALL	**11,671**	**72%**	

Individual country research findings published at:
http://www.gsma.com/publicpolicy/mobile-and-privacy/resources

For further information contact:

Yiannis Theodorou
mobileprivacy@gsma.com

GSMA Head Office

Seventh Floor, 5 New Street Square, New Fetter Lane, London EC4A 3BF UK

Tel: +44 (0)207 356 0600

www.gsma.com