



CLICK WITH CONFIDENCE

# Mobile Privacy: A User's Perspective

## *Summary Findings*

Prepared by: Harris Interactive  
April, 2011

# Table of Contents

## Introduction and Executive Summary 2

- Background and Objectives
- Methodology
- Executive Summary

## Detailed Findings 9

- Privacy and Information Sharing
- Social Networking and Advertising on Mobile
- The TRUSTe trust mark



CLICK WITH CONFIDENCE

# Executive Summary

# Background and Objectives

## Background

TRUSTe offers companies a privacy certification program to help build customer trust regarding the privacy of mobile applications or mobile web sites. The features of this mobile privacy certification include:

- Privacy certifications of mobile apps and/or mobile web sites
- Graphical, short notice privacy policies optimized for mobile devices
- A mobile privacy seal & validation page optimized for mobile devices
- Enhanced privacy disclosures to address concerns unique to the mobile platform
- Privacy dispute resolution services so users can provide privacy feedback

## Research Objectives

TRUSTe would like to expand their understanding of smartphone consumer attitudes and perceptions about privacy issues related to using applications on their mobile devices. Key business questions addressed include:

- How smartphone users feel about their privacy on a mobile device
- Specific elements smartphone users are most concerned with
- Precautions smartphone users take to protect their privacy
- Reaction to/impact of a “trust mark” provided by TRUSTe

# Methodology

## Who

1,000 total interviews were conducted among Harris Interactive's online consumer panel

Respondents were qualified as:

- US residents
- Age 18 and over
- Currently own/use a smartphone
- Not employed in advertising, marketing research, telecom

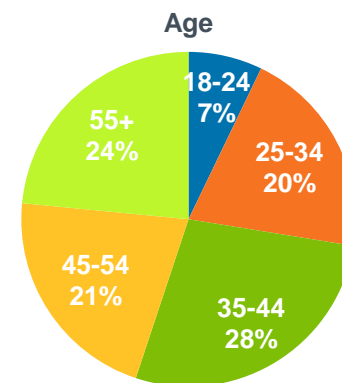
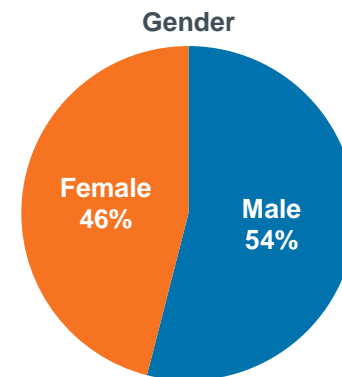
## When

Interviews were conducted February 3-17, 2011

## How

Via self-administered online survey

Weighted Representation

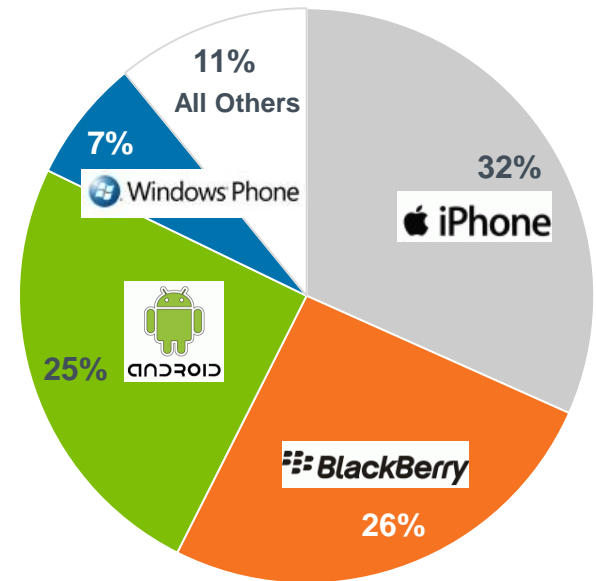


# Executive Summary

## The Smartphone Market

- The most commonly used smartphone OS brands are iPhone, BlackBerry, and Google Android, though there are indications this trend could be changing.
  - Relatively new to the market, Google Android smartphones are capturing an even larger share among new entrants to the smartphone market at the expense of BlackBerry (and iPhones to a lesser extent).
- Nine in ten smartphone users have downloaded at least one application for their phone.
- Users spend the greatest percentage of their smartphone time making phone calls (36%), although texting (19%), emailing (14%), surfing the web (7%), playing games (7%), and social networking (6%) are also common activities done on a smartphone.

Smartphone Type Use

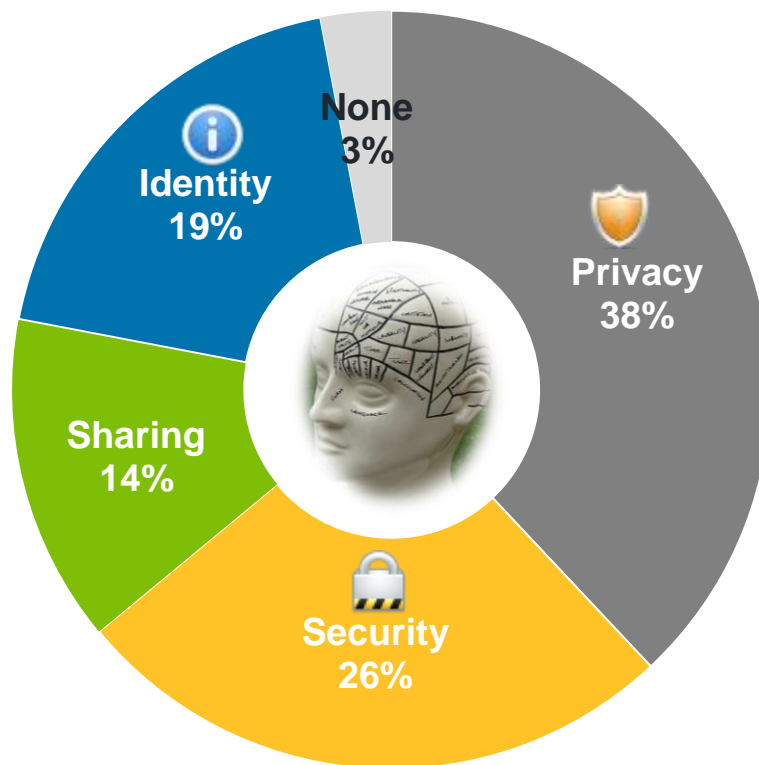


# Executive Summary

## Mobile App Privacy, Security Attitudes

- **Privacy, even more than security, represents a significant concerns for a majority of smartphone users.**
- **Privacy concerns rank #1:** Most consumers expressed great concern about their data privacy both when using smartphones in general, and when using mobile apps in particular; this concern increases with the age of the user.
- **Consumers want more control over their data:** 98% of consumers expressed a strong desire for better controls over how their personal information is collected and used via mobile devices and apps.
- **Advertising tracking causes significant concern:** Nearly three-quarters of consumers are uncomfortable with the idea of advertiser tracking, and 85% want to be able to opt into or out of targeted mobile ads.
- **Location tracking turns users off:** A significant majority (77%) of consumers doesn't want to share their location data with app owners / developers.

Primary Concern When Using Mobile Apps



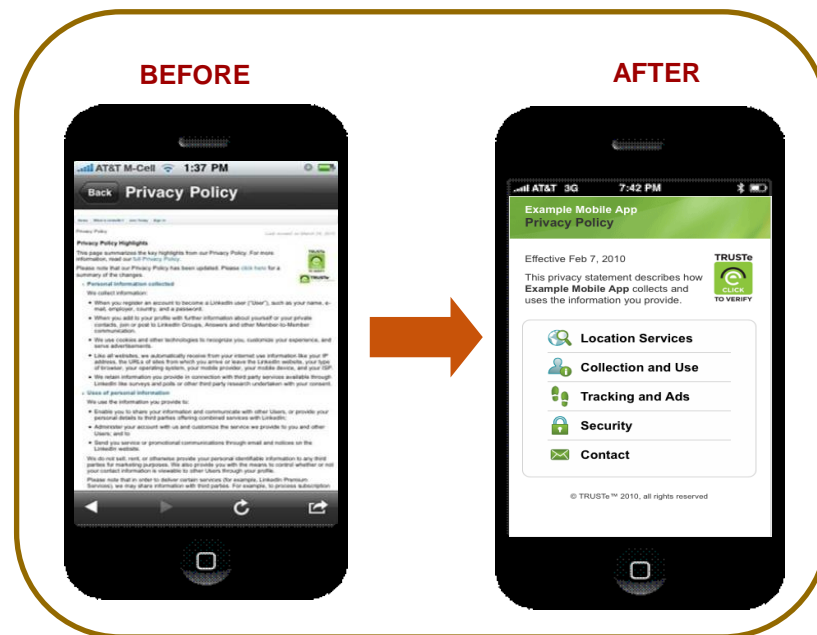
# Executive Summary

## Mobile App Privacy Behaviors

- **A majority of users do not currently feel they are in control of their personal information, but that doesn't prevent them from trying.**
  - Even in exchange for money, nine in ten would not be willing to share photos, contact lists, or surfing behavior. Some would consider sharing other types of information with a first party.
  - 98% indicate that having easy access to controls regarding the sharing of personal info in a mobile app is important.
  - The most common preventative action taken is to create strong passwords.
- **Though privacy is widely deemed important, incidence of reading privacy policies is more limited due to readability issues**
  - About one-half of smartphone users have read the privacy policy of a mobile app.
  - Four in ten claim to read and understand disclosures regarding the use of their personal information before using an app (note: those aware of TRUSTe are significantly more likely to have taken this action).
  - Recognition that app stores offer applications that safeguard privacy is also limited.

# TRUSTe's mobile privacy certification helps address critical consumer privacy issues

- **High consumer privacy concerns with Mobile Apps**
- **Unique privacy issues:**
  - Use of geo-location technology
  - Uniquely sensitive personal information (i.e. phone number)
  - Social networking increasingly relies on mobile apps
  - Lack of transparency in how applications use & transmit data
  - Privacy concerns regarding behavioral tracking for advertising purposes
- **Small-screen form factor constraints presentation of privacy practices and consumer choice mechanisms**
  - Optimized for the mobile device
  - Easier for consumers to understand
  - Enhanced disclosures to address concerns unique to mobile platform





CLICK WITH CONFIDENCE

# Detailed Findings

Privacy and Information Sharing

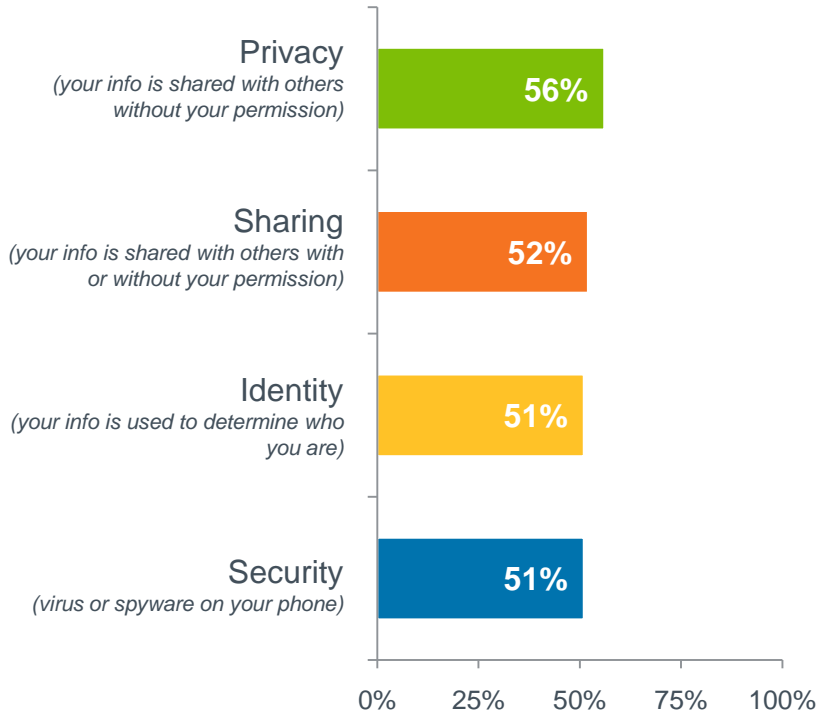
Social Networking and Advertising on mobile

The TRUSTe Trust mark

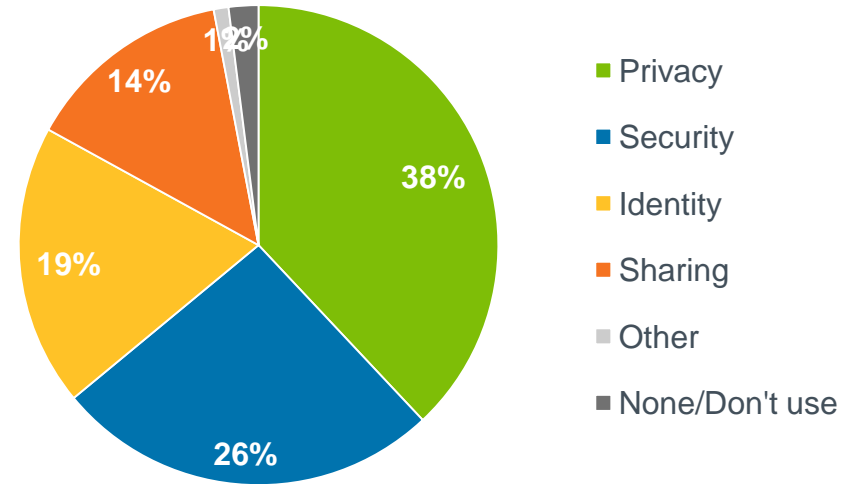
Mobile app concerns are similar to smartphone concerns in general. When asked to choose only one, privacy is deemed the most important issue, across user groups.



**Mobile App Concerns**  
(% Top 3 Box/10-Point Scale)



**Primary Mobile App Concern**



BASE: Total Qualified Smartphone Users (n=1000)

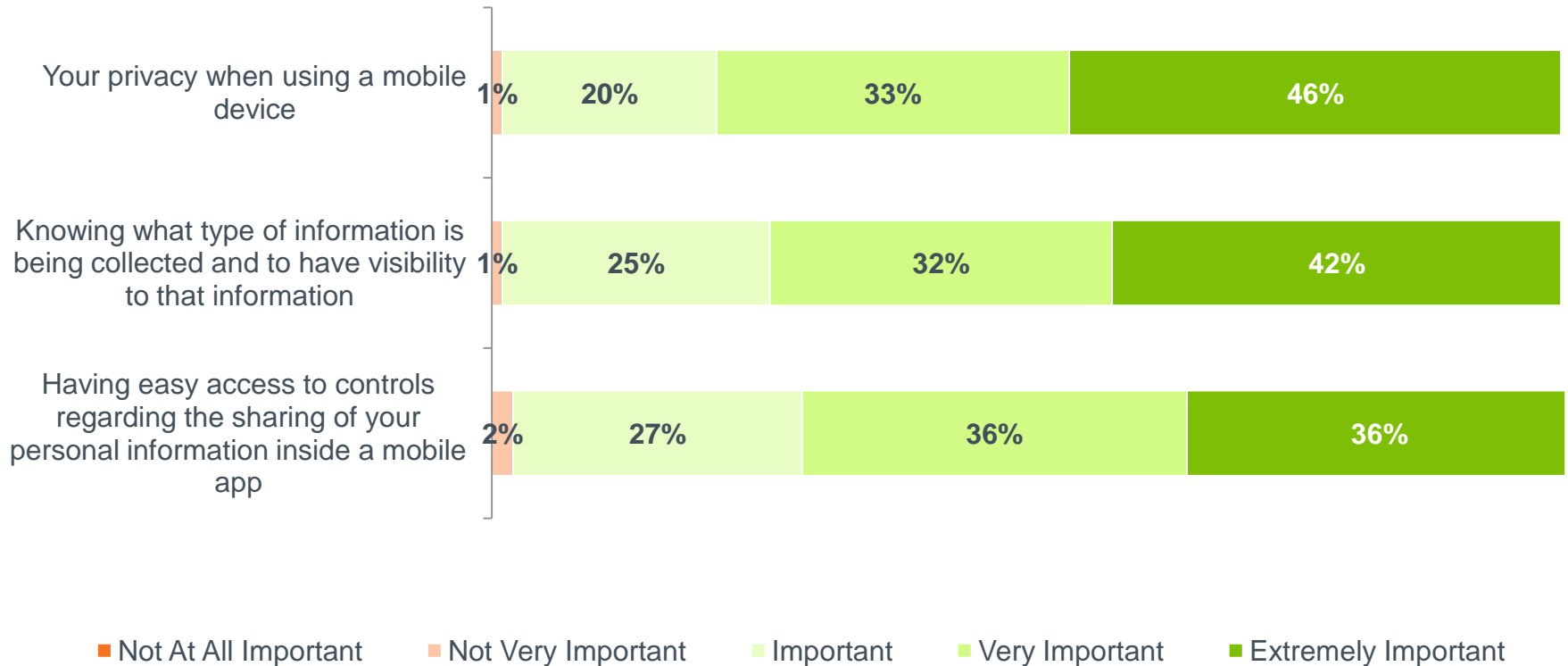
Q811 And, how concerned are you about each of the following when using mobile applications?

Q815 Which of the following is your primary concern when using mobile applications?

Nearly all agree privacy is an important issue when using a mobile device, as is knowing what type of information is collected and the ability to control what is shared.



### Importance of...



BASE: Total Qualified Smartphone Users (n=1000)

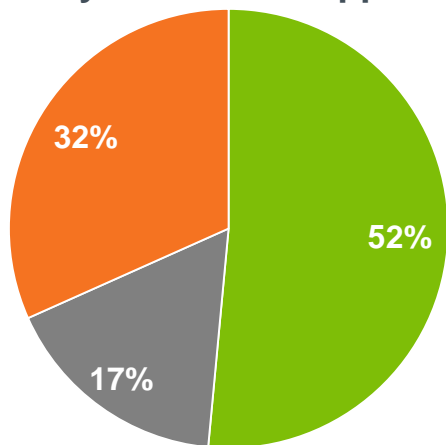
Q946 How important is it know what type of information is being collected and to have visibility to that information?

Q951 How important is your privacy when using a mobile device?

Q1031 How important is it to have easy access to controls regarding the sharing of your personal information inside a mobile app?

About one-half (52%) claim to have read the privacy policy of a mobile app, most commonly on the app itself.

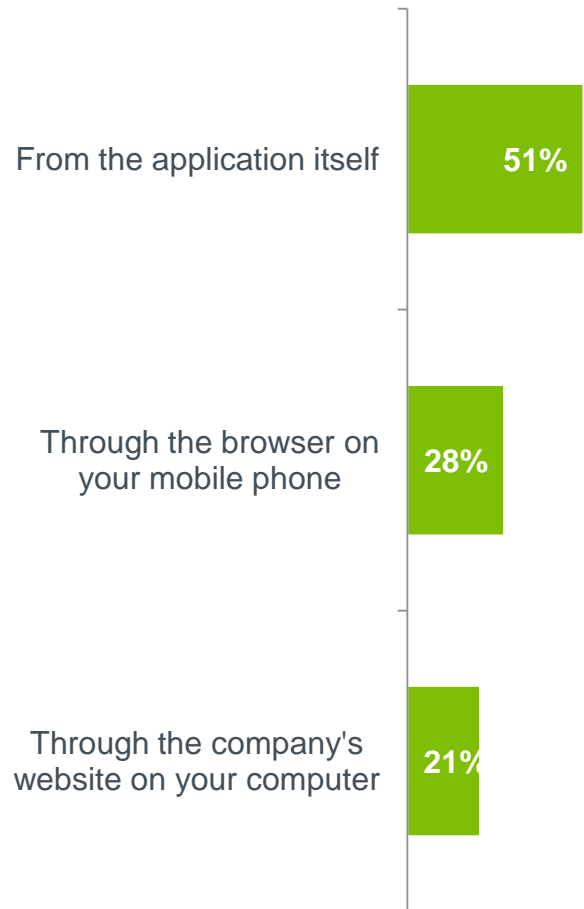
### Have you ever read the privacy policy of a mobile app?



- Yes
- No, I have never seen an app with a privacy policy
- No, I have not read the privacy policy



### Where have you checked the privacy policy of a mobile app?



BASE: Total Qualified Smartphone Users (n=1000)

Q1010 Have you ever read the privacy policy of a mobile app?

BASE: Those who have checked the privacy policy of a mobile app (n=523)

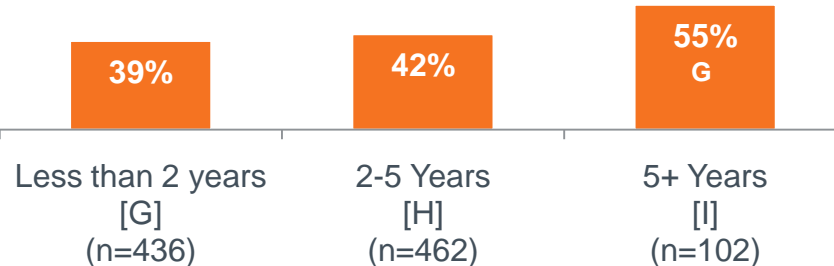
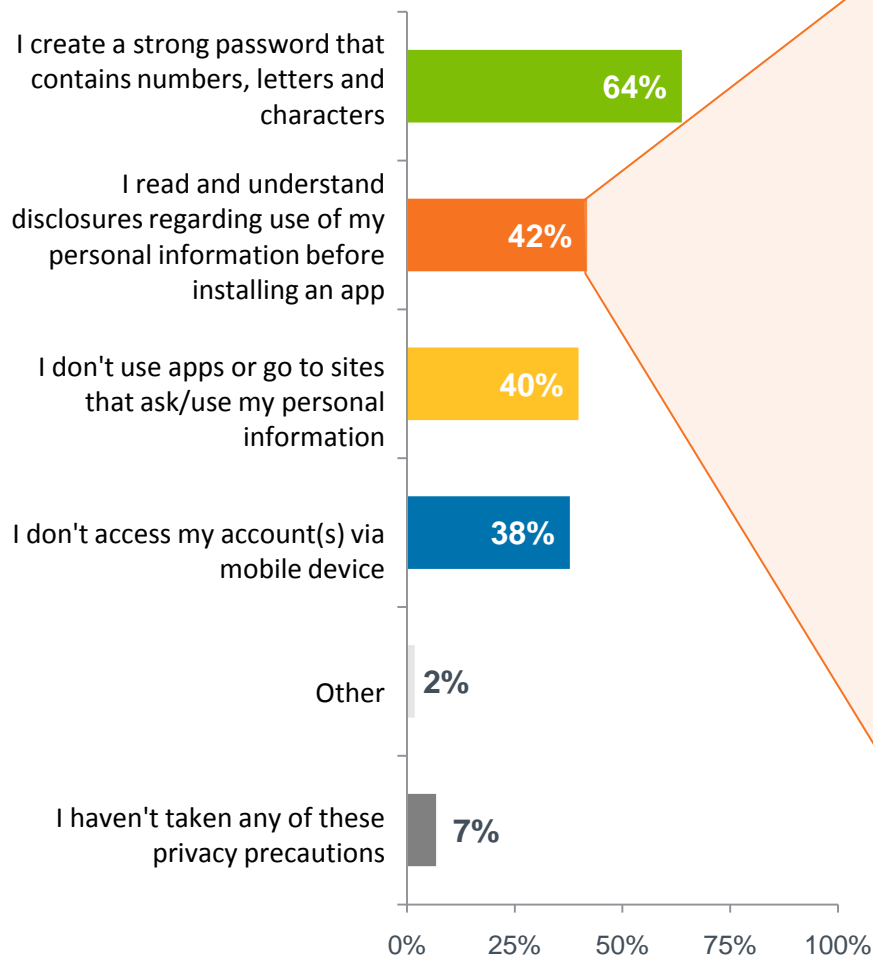
Q1015 Where have you checked the privacy policy of a mobile app?

**Strong passwords are the most commonly taken privacy precaution. About four in ten indicate they read disclosures – an action more common among long tenured users, those aware of TRUSTe, and those who download mobile apps. Some don't use Apps or access their Accounts**

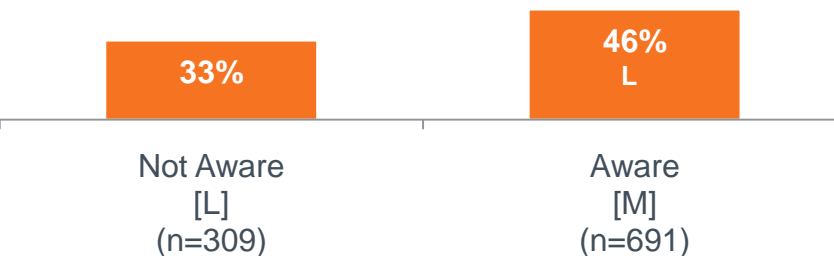


**Differences By Length of Smartphone Use**

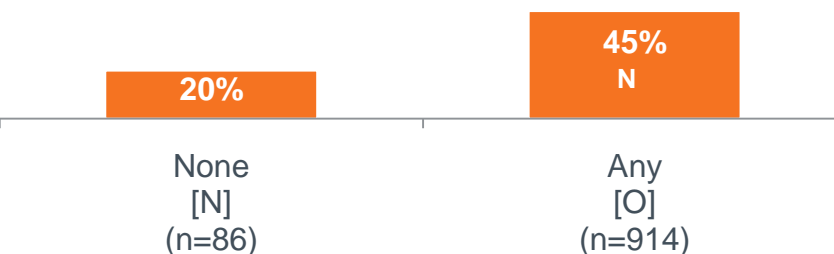
**Privacy Precautions Taken**



**Differences By TRUSTe Awareness**



**Differences By Application Downloads**



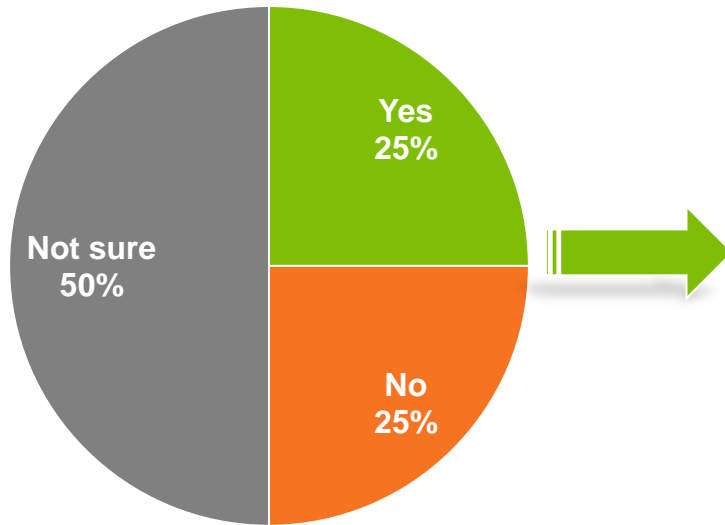
BASE: Total Qualified Smartphone Users (n=1000)

Q820 Which, if any, of the following privacy precautions do you take with regards to your online accounts?

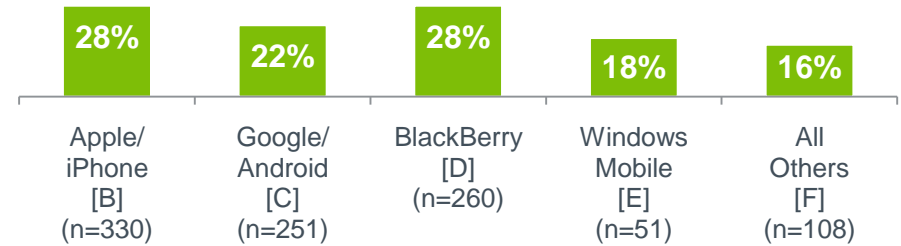
A minority (25%) feel their mobile app store makes available apps that safeguard privacy, though nearly four in ten (38%) are confident that the apps themselves do protect privacy.



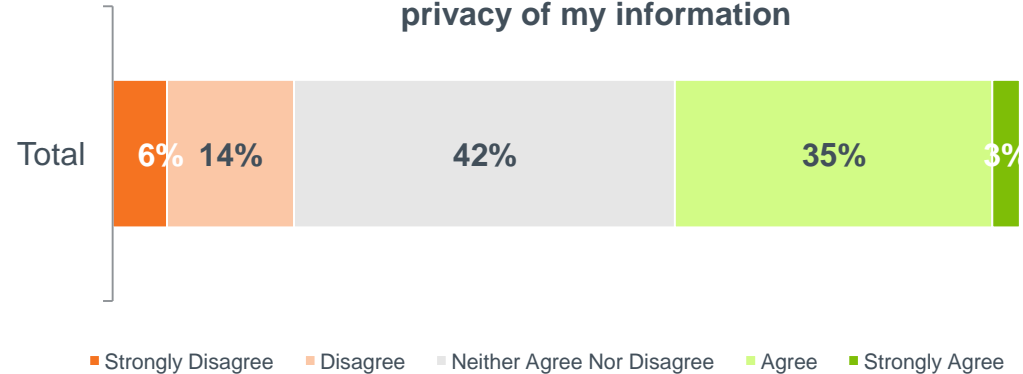
Does your mobile app store make available only apps that safeguard your privacy?



Differences By Type of Smartphone Used (% Yes)



I feel confident that most mobile apps protect the privacy of my information



BASE: Total Qualified Smartphone Users (n=1000)

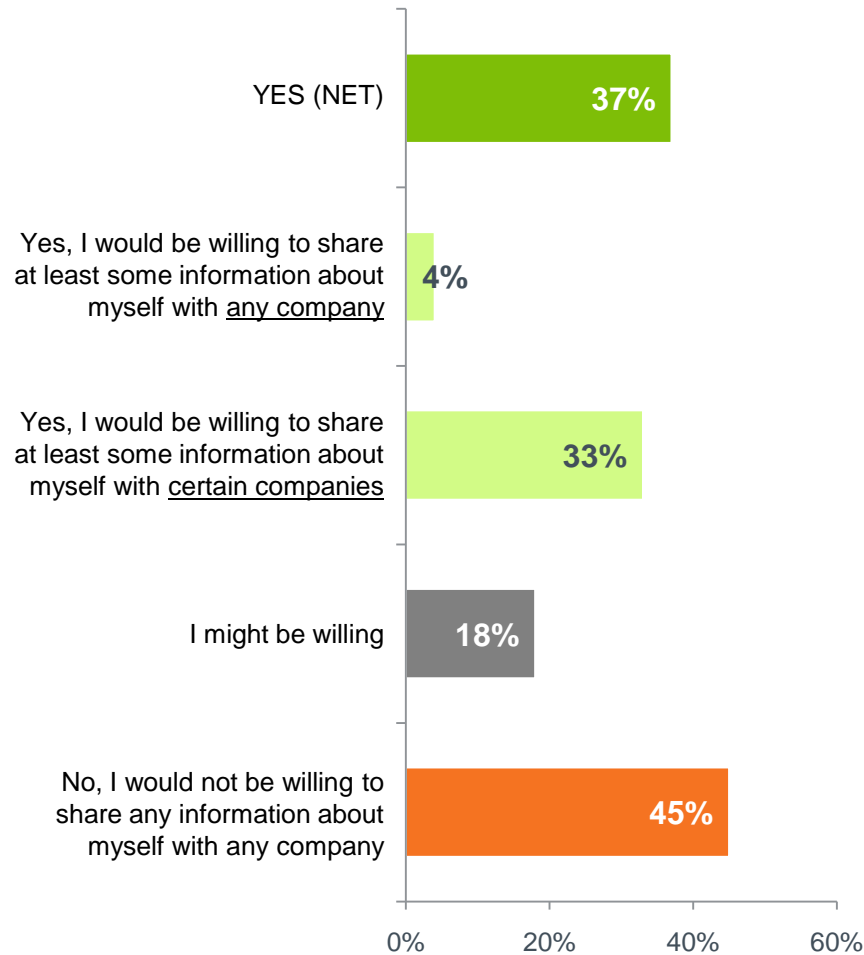
Q825 Do you feel that the mobile application store you use only makes available apps that safeguard the privacy of your information?

Q831 How much do you agree or disagree with the following statement? - I feel confident that most mobile apps protect the privacy of my information

About four in ten would be willing to share personal information in exchange for a free or lower cost mobile app, although there are limitations (only certain information to certain companies).



### Willingness To Share Personal Info



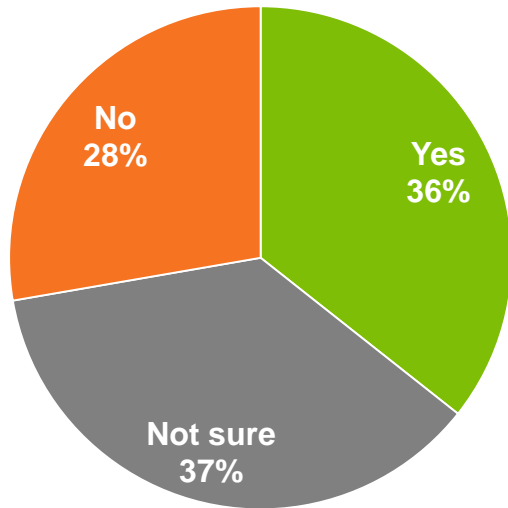
BASE: Total Qualified Smartphone Users (n=1000)

Q905 Are you willing to share any personal information with a company in exchange for a free or lower cost mobile app?

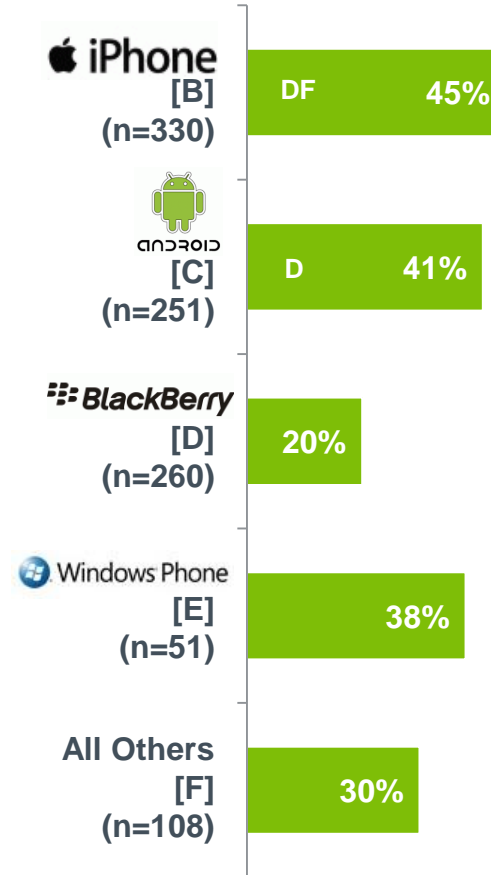
A minority feel they have a choice regarding the collection and use of location information, though the incidence is higher among iPhone and Android smartphone users.



Do you feel you have a choice regarding the collection and use of your location information by an application? 🚩



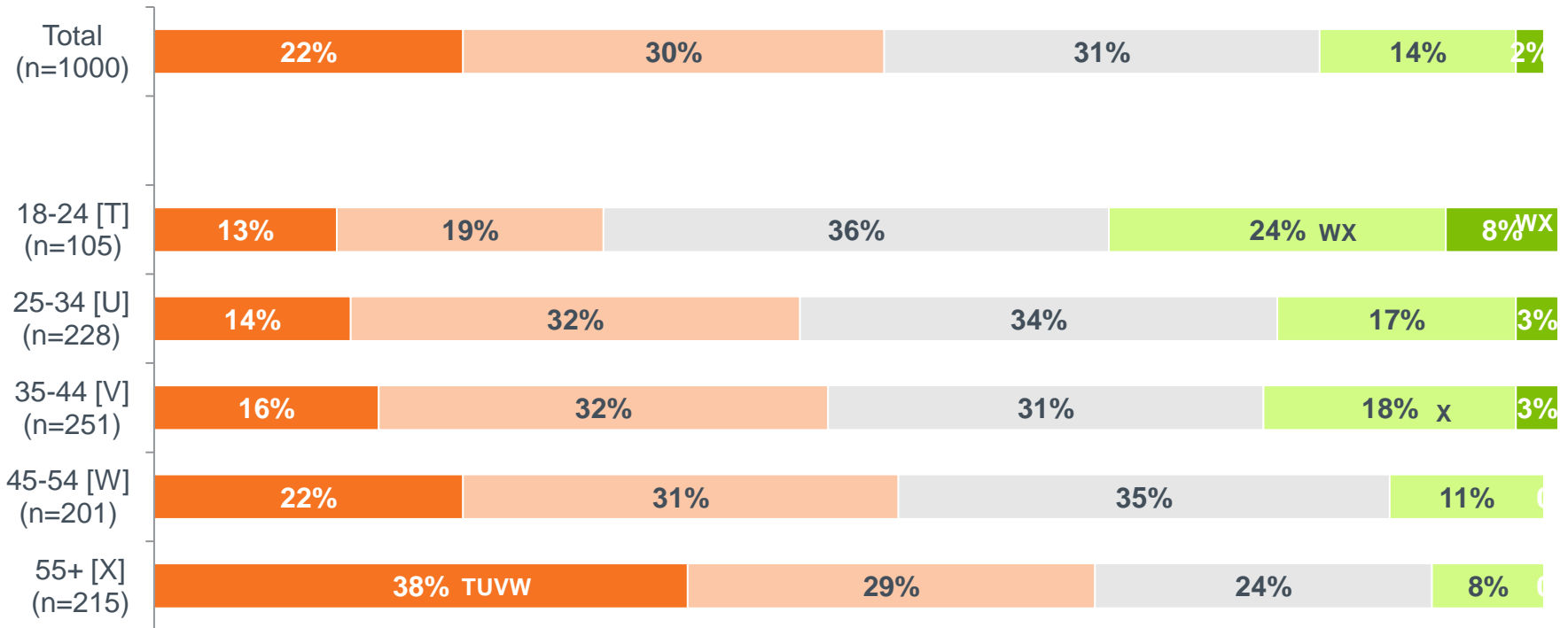
Differences By Type of Smartphone Used



A majority (52%) are uncomfortable with the idea of signing in to other applications with another account ID, such as Facebook or Twitter.



### Comfort Level With Signing In To Other Applications or Websites With Your Facebook, Twitter, or Other Account ID



■ Very Uncomfortable 
 ■ Uncomfortable 
 ■ Neither Comfortable Nor Uncomfortable 
 ■ Comfortable 
 ■ Very Comfortable

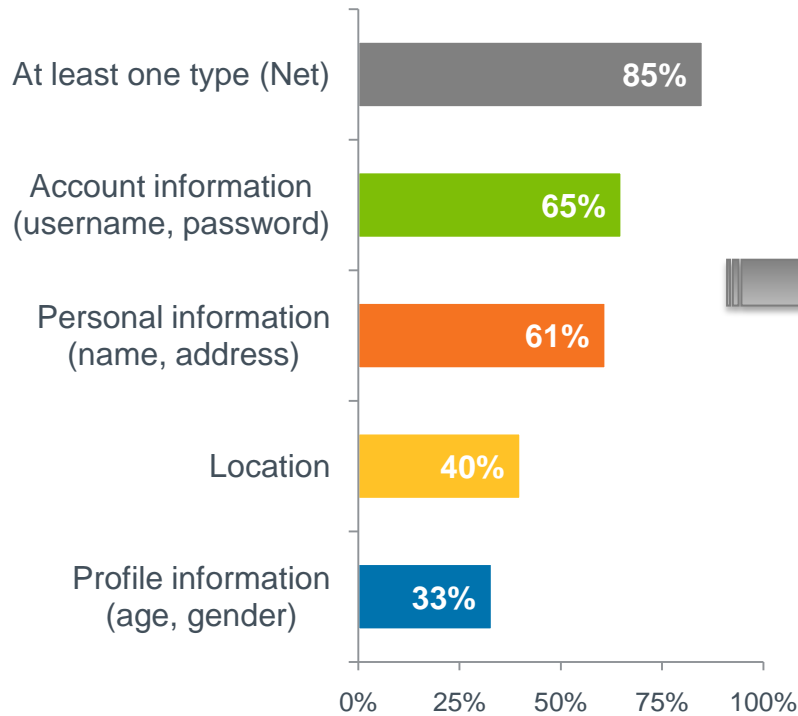
BASE: Total Qualified Smartphone Users (n=1000)

Q941 How comfortable do you feel signing in to other applications or websites with your Facebook or Twitter account or other ID compared to registering with the application directly/creating an account for just that app or company website?

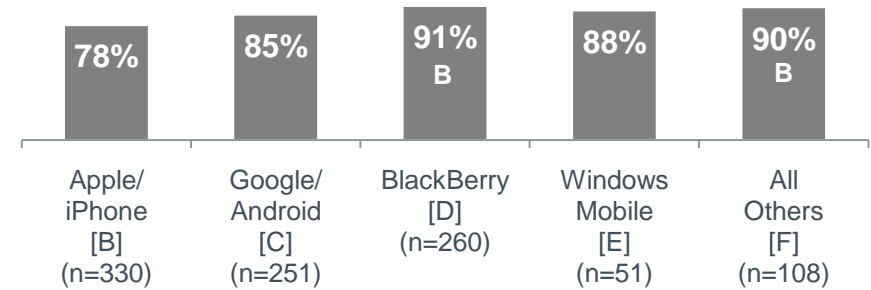
# Nearly nine in ten (85%) restrict at least some types of information sharing on mobile apps



## Information Would Not Share Through A Mobile App



## Differences By Type of Smartphone Used



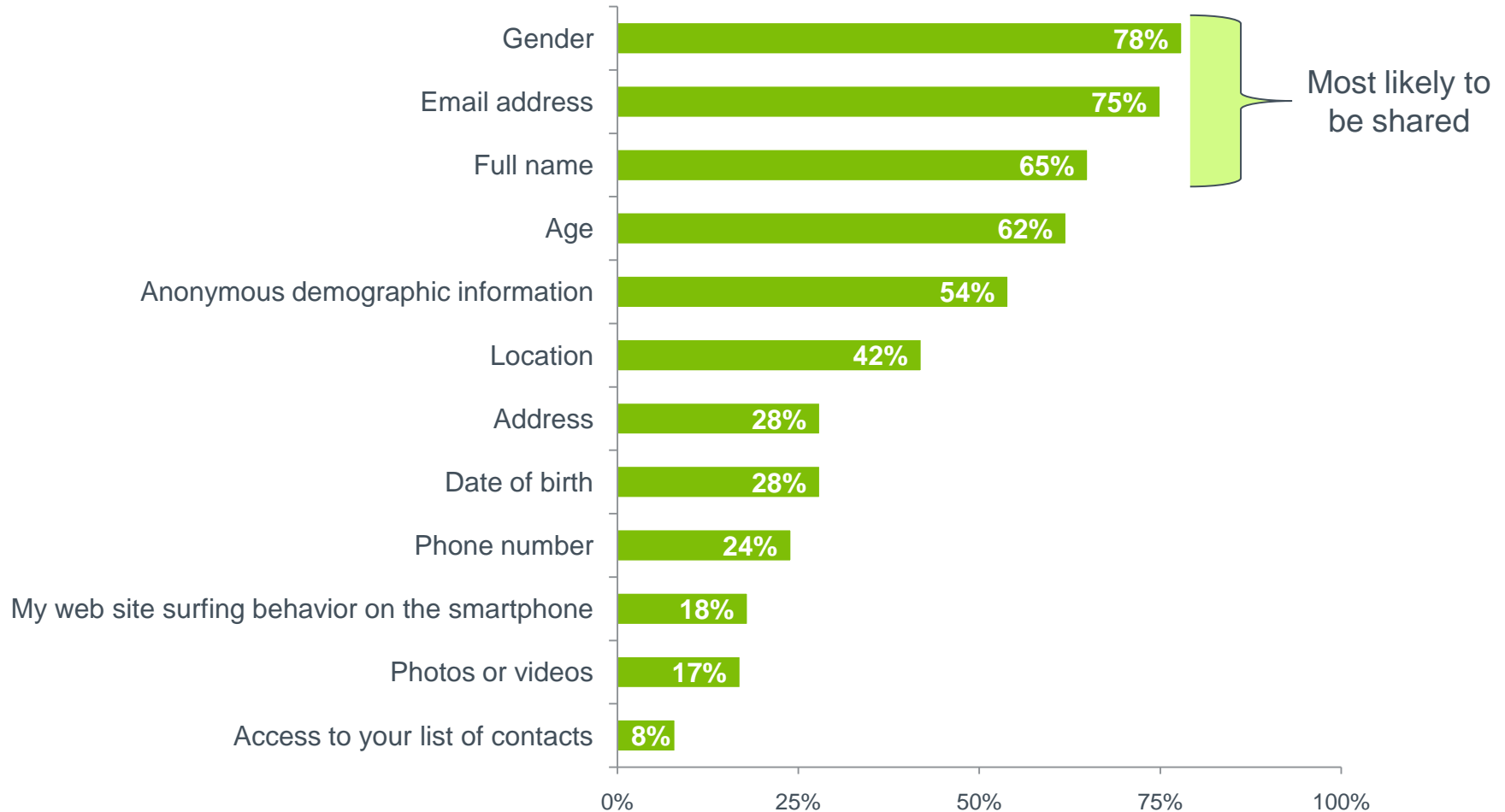
BASE: Total Qualified Smartphone Users (n=1000)

Q900 Are there certain kinds of information you do not share through a mobile app?

Among those who indicate they might be willing to share personal information, gender, email address, and name are the most likely to be shared.



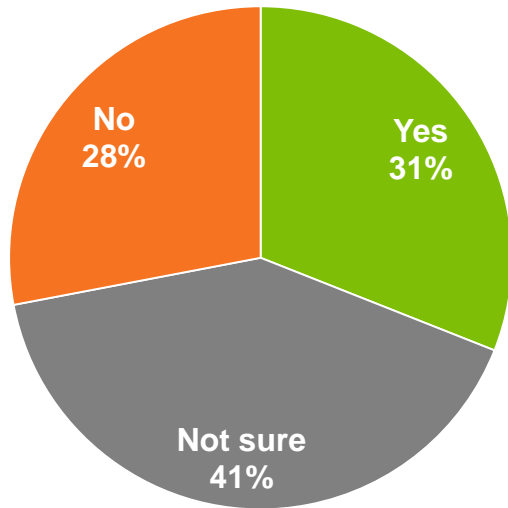
### Types of Information Willing To Share With Either A First Party App Owner/Developer Or A Third Party



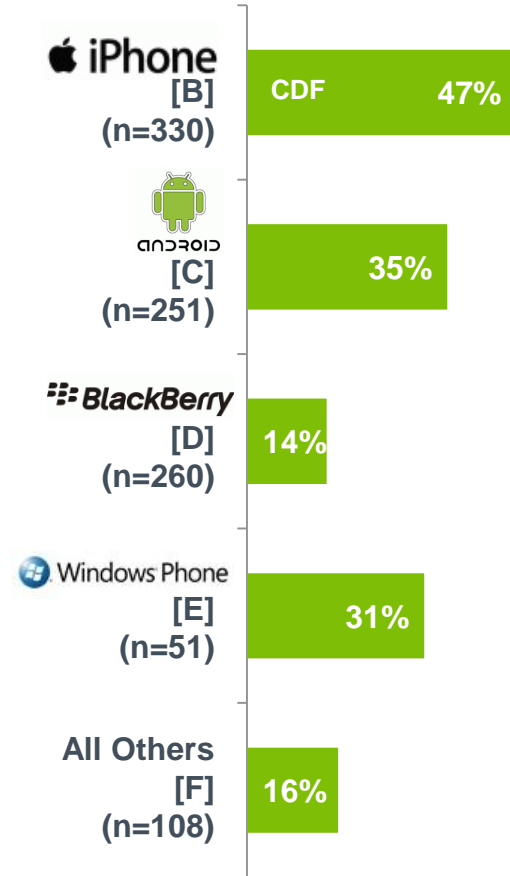
Overall, about one-third indicate their smartphone alerts them when location information is being collected; this is significantly more common among iPhone and Android users.



Does your smartphone alert you when location information is being collected? 🚩



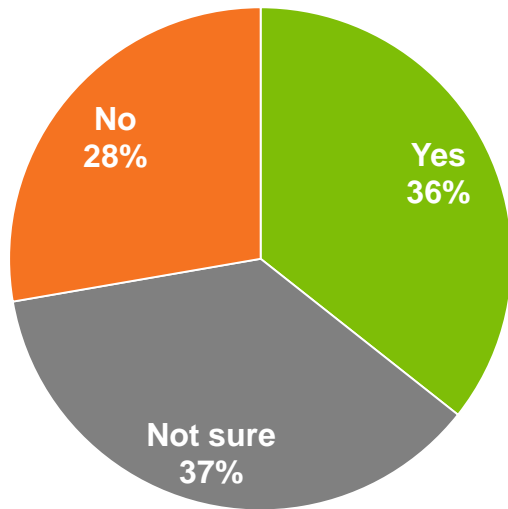
Differences By Type of Smartphone Used



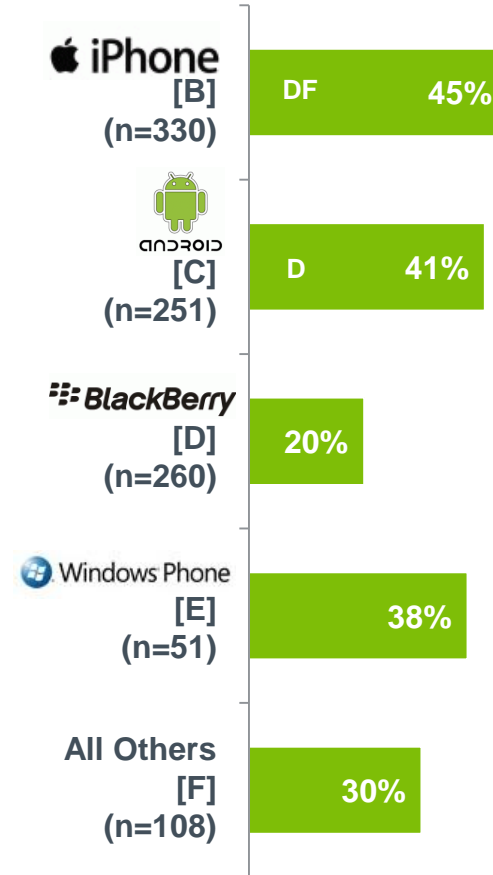
# A minority feel they have a choice regarding the collection and use of location information, though the incidence is higher among iPhone and Android smartphone users.



Do you feel you have a choice regarding the collection and use of your location information by an application? 🚩



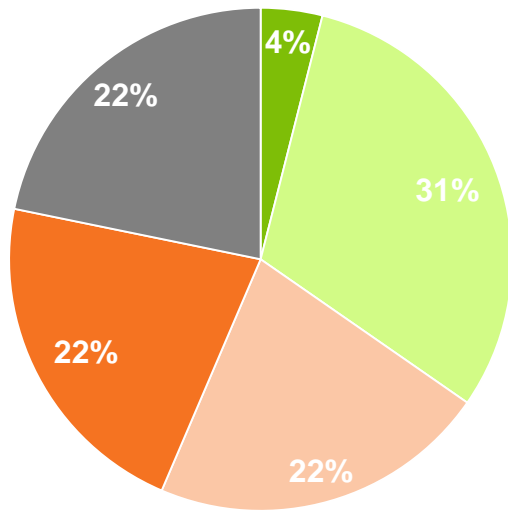
Differences By Type of Smartphone Used



About one in three smartphone users allow an app access (at least sometimes) to their location information; more than one-half of iPhone users allow location access.



If an application asks for your location information, what do you typically do?

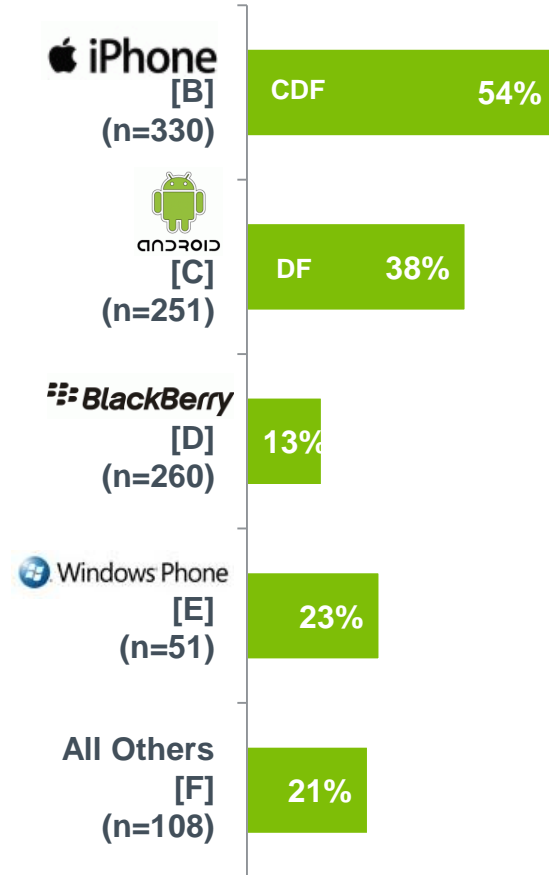


Net: Allow 35%



- Always allow access
- Sometimes allow access
- Rarely allow access
- Do not allow access
- I have never had an application ask for my location

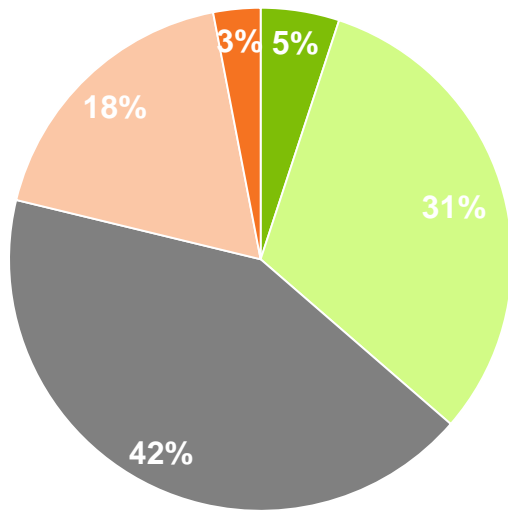
Differences By Type of Smartphone Used



# Only about one-third feel they are in control of their personal information when using a mobile device.



## I Feel In Control of My Personal Information When Using My Mobile Device

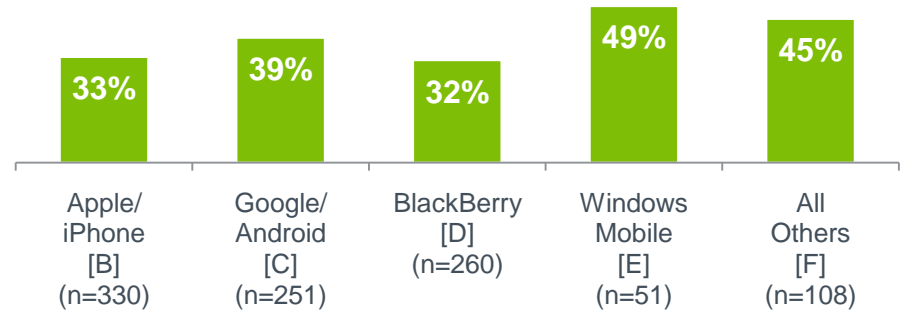


- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

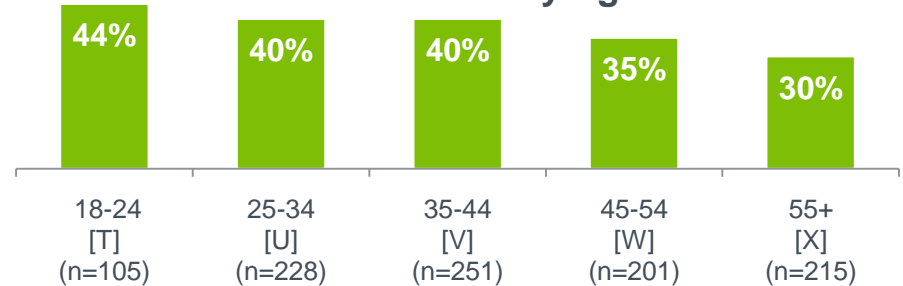
Net:  
Agree  
37%



### Differences By Type of Smartphone Used



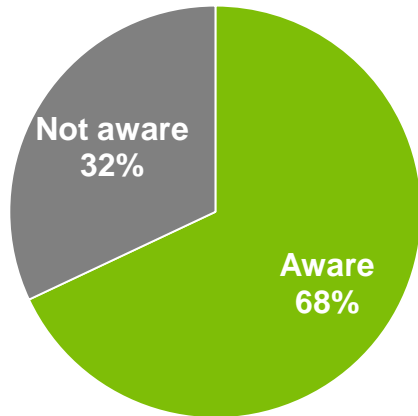
### Differences by Age



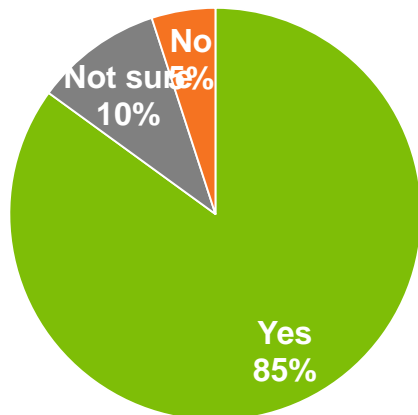
A majority (74%) of smartphone users are not comfortable with the idea of advertiser tracking and 85% are interested in being able to opt in/out of targeted mobile ads.



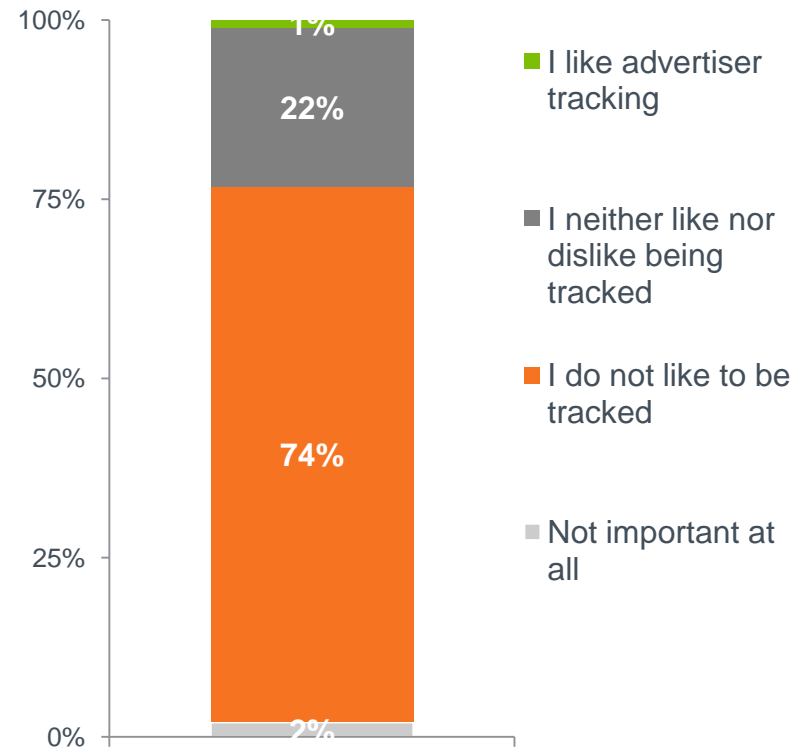
Are you aware that advertisers are tracking your mobile activities and delivering ads targeted to you based on your behavior?



Are you interested in being able to opt in or out of targeted mobile ads?



Feelings About Advertiser Tracking



BASE: Total Qualified Smartphone Users (n=1000)

Q1040 Are you aware that advertisers are tracking your mobile activities and delivering ads targeted to you based on your behavior?

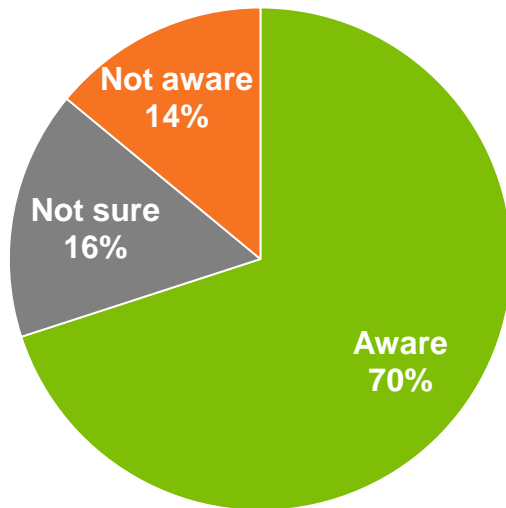
Q1045 How do you feel about being tracked by advertisers on your mobile phone?

Q1050 Are you interested in being able to opt in or out of targeted mobile ads?

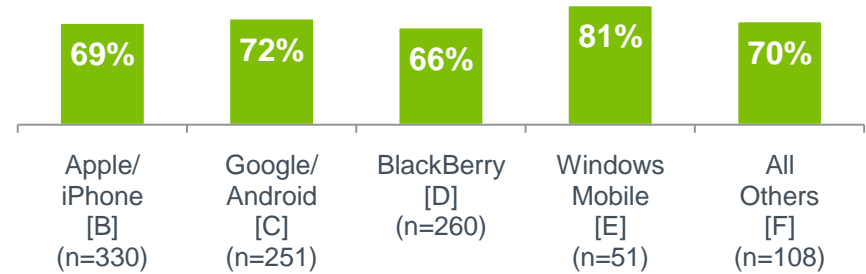
Fully seven in ten claim to have seen the TRUSTe mark before; awareness is significantly higher among men and among those who download mobile apps.



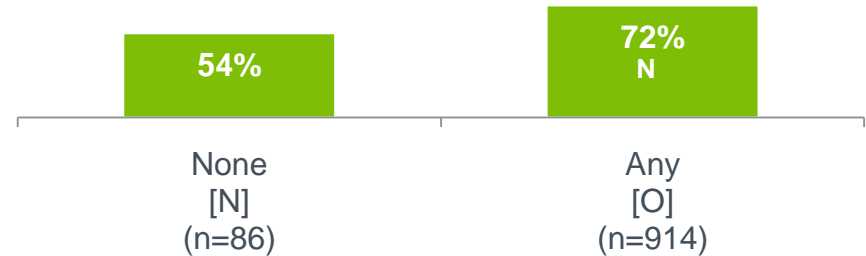
### Aware of TRUSTe Mark



### Differences By Type of Smartphone Used



### Differences By # of Apps Downloaded



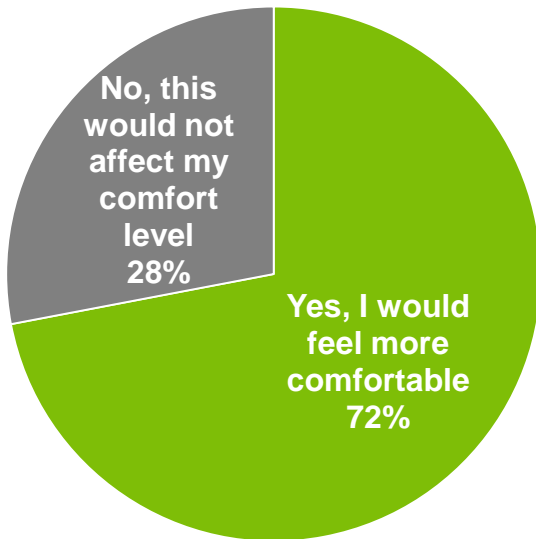
BASE: Total Qualified Smartphone Users (n=1000)

Q1051 Have you ever seen this trust mark or seal before today (on mobile apps, mobile websites, or traditional PC websites)?

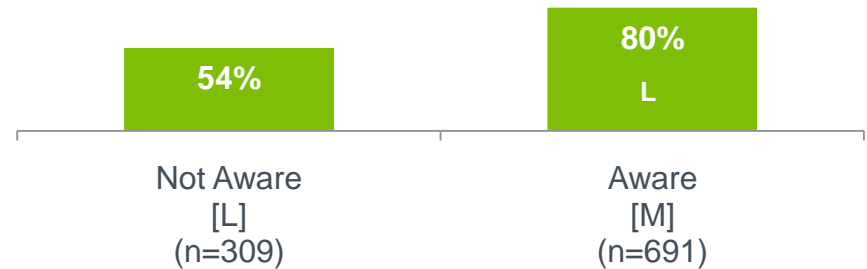
The TRUSTe mark increases the comfort level smartphone users feel about their privacy, even among those who had not heard of it before.



### Impact of TRUSTe Mark On Comfort Level



### Differences By TRUSTe Awareness



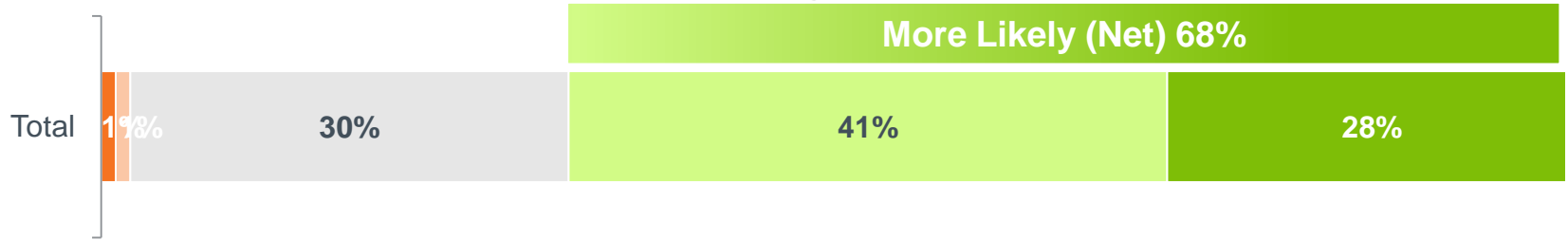
BASE: Total Qualified Smartphone Users (n=1000)

Q1055 If you saw this trust mark or seal on a mobile app or mobile web site or store would you feel more comfortable about your privacy on that site?

The short-notice privacy policy with the TRUSTe logo is preferred by a large margin. About seven in ten indicate they would be more likely to read a privacy policy that is easier to navigate/read.



### Likelihood To Read Privacy Policy That Is Easier to Navigate and Read



- Much Less Likely to Read
- Less Likely To Read
- About the Same
- More Likely To Read
- Much More Likely To Read



7% Prefer



90% Prefer



3% Prefer

BASE: Total Qualified Smartphone Users (n=1000)

Q1021 How much more likely would you be to read a company's privacy policy (on your mobile phone) if it was easier to navigate and read?

Q1025 Which of these privacy policies would you prefer to read?

**For the detailed survey  
results or to learn more about  
mobile privacy, go to  
<http://www.truste.com/harris-mobile-survey/>**