

# Building a Trusted Mobile Strategy: Increase User Trust to Further your Mobile Platform Strategy

As mobile growth continues, an increasing number of companies are creating mobile applications and mobile-formatted websites. Consumers' use of mobile apps and websites, however, is hindered by the perception that mobile devices are less safe and secure than home computers. Consumers are hesitant to share personal and financial information with mobile websites and applications. A recent KPMG survey found that 87 percent of consumers who refrain from mobile banking do so out of concern for their security and privacy<sup>1</sup>. Consumers have privacy concerns unique to the mobile device and its capabilities: a recent survey found that 52 percent of mobile users are "very or extremely concerned" about a loss of privacy from using location-aware mobile applications<sup>2</sup>.

Successful companies must recognize this trend and adapt, simultaneously satisfying consumer demand for mobile sites and services as well as pacifying consumer concerns over mobile privacy and security.

This paper outlines the mobile landscape and introduces best design and privacy practices for mobile applications and websites, location-aware technologies, and mobile advertising. TRUSTe has helped thousands of companies in the area of online privacy since 1997. With a wide range of privacy seals and services, TRUSTe is well-positioned to help businesses build trust on the mobile platform. With more trust, users and customers will be more inclined to download your app, register for new accounts, and make purchases via your mobile app or website.

## Mobile Architecture Considerations

Given explosive mobile growth companies are no longer asking whether they should create mobile offerings, but how to best adapt their products and services in the mobile platform. Companies are developing both mobile apps and mobile-formatted versions of their traditional websites. A mobile app is a piece of software that runs directly on a user's mobile device whereas a mobile website is simply a website tailored to small mobile screen sizes, offering app-like UI and often incorporating mobile technology like location awareness.



1. <http://www.prnewswire.com/news-releases/kpmg-survey-mobile-banking-steadily-gaining-acceptance-among-us-consumers-99013114.html>

2. <http://www.poynter.org/column.asp?id=134&aid=186560>

Domino's Pizza, for example, has a mobile-optimized website that recognizes a user's location via GPS and allows customers to order food via a mobile menu with intuitive buttons. Your company's ideal mobile presence will depend on your product, strategy, and objectives. For example, companies in the gaming and entertainment industries such as EA, the NFL and Yelp tend to favor mobile apps, while companies in the commerce and social networking industries generally favor mobile websites.

If your company decides to create an app, consider the cost and maintenance involved in developing applications for each mobile operating system (OS). Recognize that different platforms may have different technical standards and revenue terms. Leading mobile platform providers include Android, Apple, Blackberry, Microsoft Windows, Palm and Symbian. While the iPhone is extremely popular, creating an iPhone-only application can alienate a large number of consumers as the iPhone is only expected to account for 10% of all mobile devices sold in 2010. In addition, OS and platform marketshare may vary by country. Because of the burden of engineering across different mobile platforms, analysts predict that mobile websites (which are not OS specific) will grow faster than mobile applications.

**If your company decides to create a mobile website you have several options to consider, including:**

1. A mobile version of your existing website offering the same features as your traditional site, but formatted for the smaller screens of mobile devices.
2. A plug-in-based mobile site. Similar to mobile websites, blogs and websites based on WordPress, Drupal, or similar open-source platforms can use free plug-ins, which automatically format sites for mobile audiences.
3. A mobile landing page. As the name suggests, a single-page entity can be created quickly to add a mobile-Web presence to a marketing campaign.
4. A dedicated mobile site. This standalone, multi-page entity, is not merely a mobile-formatted version of your traditional website, but a fully functional website with mobile design, messaging and functionality.

## Mobile Design Considerations

Building a successful mobile app or website requires not only creativity and innovation, but also solid design principles. Tasks performed on mobile devices tend to be tactical in nature: users have a very specific need and want to fulfill it in the easiest and fastest way possible. Design your mobile app or website with the following principles in mind:

- Compact mobile screen sizes require a minimal feature set optimized for common needs and tasks.
- Fonts and font sizes should be used to show hierarchy and importance.
- The ability to only see one screen at a time means features must be progressively displayed.
- Large buttons should be used to make choices easily actionable.
- Limited screen real estate makes help text or FAQs impractical - your mobile interface should be so simple and intuitive that it does not require explanation.

Smart mobile design is a prerequisite to entry, not a guarantor of success - users are presented with dozens, if not hundreds of similar, competing mobile websites and applications. Your company needs to stand out from the crowd, but how? Addressing users' concerns about mobile privacy and security in your mobile app or website is an excellent way to differentiate yourself from competitors and accelerate business.

### OPTIMIZE YOUR SITE/APP FOR MOBILE USE



### Build User Trust with a Mobile Privacy Policy

A December 2009 study by TNS Global Market Research revealed that more than 75% of users look for the presence of a privacy policy when providing personal information on a website. Having a mobile-optimized privacy policy will help your users feel more comfortable providing their personal information on your mobile website or application. For example, when a user first downloads an application you can place a link to your privacy policy in a visible location to immediately alleviate consumer concern.

Excessive length and complicated language can diminish the impact of a privacy policy and this is especially true on the mobile platform where space is at a premium and ease-of-use is a must. Consider the following guidelines for designing your mobile privacy policy.

- Use icons to help users quickly identify the key components of your privacy policy. The icons should be relevant to the subject matter and not be selected for the sake of providing an icon.
- Progressively display privacy notices to avoid information overload. The first screen of your privacy policy can contain a summary of the policy's key components and often that summary is sufficient to satisfy a user's concern.
- Don't forget to provide the user with access to the complete privacy policy, which can be accomplished with a hyperlink, embedded in the short privacy notices in the mobile interface.

Reduce the time a user must spend understanding and feeling comfortable with your privacy practices and your will increase the time users spend interacting with your mobile website or app.

### ICONS HELP QUICKLY IDENTIFY KEY COMPONENTS



### Navigating User Privacy Concern with Location Awareness Technology

Many mobile devices sold today come equipped with location-aware technology, capable of pinpointing users within 30 feet of their actual location. This technology has been harnessed by mobile apps in a variety of useful and innovative ways – from social apps that allow users to locate their friends when they’re out and about (like Foursquare) to photo apps that geo-tag pictures (like Hipstamatic) for later reference. Location awareness is also a way for marketers to target offers and advertisements to consumers through increased relevance, accuracy, and timeliness.

However, consumers are predictably wary about the implications of sharing their location information with mobile websites and apps. A recent survey by Webroot found that more than half of location-enabled mobile users are worried about a loss of privacy.<sup>3</sup> They’re concerned about who collects this data, who can see it, how long the data is stored, and its potential use by marketers. The harms consumers risk from unintentional breaches of this data include annoyance, embarrassment and most seriously, danger to person or property.

**To successfully incorporate location-aware mobile technology into your products or services, consider the following best practices:**

1. Provide users with transparency and remain accountable– use clear messaging to help users understand how their location data will be used and shared. Provide security for this data through means such as encryption, and ensure that adequate consumer redress mechanisms exist for consumers who want to remove their location data from your databases.
2. Provide users with choice – This means asking users permission to use their location information before you collect it. This choice is only meaningful when consumers understand the implications of sharing their data so again, ensure that your messaging is concise and unambiguous.
3. Have a privacy trustmark – Users will reward companies who make strong commitments to their privacy, but advertising this commitment can be difficult. Digital privacy trustmarks can effectively advertise your privacy commitment to consumers and ensure that you are rewarded for providing them with privacy protections and assurances. Users recognize that a website or application displaying an established trustmark like a TRUSTe privacy seal has undergone rigorous vetting by an independent third party and is worthy of their trust, resulting in increased downloads, registrations and purchases for websites or applications who display these trustmarks.

3. Webroot survey on July 13, 2010 of 1,500 social networking users who own geo-location mobile devices, <http://pr.webroot.com/threat-research/cons/social-networks-mobile-security-071310.html>

## Mobile Advertising: Proceed with Eyes Open

There are a lot of mobile apps that are free of charge to users. Recent estimates show that about two-thirds of apps on the Android marketplace are free and one-third are paid. The estimate is the opposite at the Apple store with one-third of the apps offered for no cost. Most of the free apps, however, are subsidized with advertising. More effective ads utilize geo-location and behavioral advertising which have privacy implications and must be implemented carefully.

Congress has taken a strong interest in protecting consumer information with regards to the use and delivery of advertising. For example, Rep. Rush introduced a bill on online privacy on July 20, 2010 called the Best Practices Act of 2010. As a result of this and Rep. Boucher's bill, Congress is currently considering federal privacy legislation that will impose additional notice obligations on companies with regards to the collection and use of personal data.<sup>4</sup> This legislation would classify geo-location data as sensitive and would require a user opt-in to use of this type of data for online advertising or marketing purposes.

Additionally, the FTC's review culminated in the agency's Self-Regulatory Principles for Behavioral Advertising.<sup>5</sup> While the Principles are not binding rules, they do provide guidance for self-regulatory efforts. The principles specifically require that companies get "affirmative express consent" when using sensitive data; furthermore, the Report classifies geo-location data as sensitive. This means that companies should strongly consider using opt-in notice for location apps - especially if the intended use is for targeted advertising or marketing efforts.

## A Comprehensive Solution: TRUSTe Mobile Privacy Certification

TRUSTe's new mobile privacy certification program allows businesses to effectively reassure their mobile customers that they can be trusted with their personal information on mobile platforms.

### Key features of TRUSTe's mobile certification program include:

- A small device-friendly privacy policy with a summary section, icon support and intuitive interfaces.
- A mobile-optimized TRUSTe privacy seal so mobile websites and apps can win consumer trust through the use of TRUSTe' respected, global privacy trustmark.
- Privacy dispute resolution services to minimize brand damage and privacy fallout.

The TRUSTe mobile privacy certification program helps companies successfully incorporate technologies such as geo-location, advertising, and social networking such as Facebook's Places for their mobile applications and mobile websites - leading to more conversions on that platform.

4. Rep. Rush introduced a bill on online privacy on July 20, 2010 called the Best Practices Act of 2010

5. FTC BA Principles Report, <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>social-networks-mobile-security-071310.html

## Learn More

Contact TRUSTe at 415.520.3490 or visit [www.truste.com/mobile](http://www.truste.com/mobile) to learn more about TRUSTe's Mobile Privacy certification.