



TRUSTe Mobile App & Mobile Web Site Privacy Certification FAQs

WHAT IS THE DIFFERENCE BETWEEN MOBILE AND TRADITIONAL WEBSITE PRIVACY CERTIFICATION?

Consumers are more sensitive to the collection & use of their information via mobile device (personal, location and device-specific info) compared to traditional web site information (personal and some PC-specific info).

Web Privacy certified companies only have their basic web site certified; additional requirements are now necessary to certify their mobile sites and apps, including;

- Testing of application behavior such as mobile technology usage (data collected, how used and how shared).
- Greater variability by platform (iPhone, Android, Blackberry are different from each other).
- Mobile apps require more frequent reviews (4 updates vs. <1/year) than PC web sites.
- Creation of additional disclosures in the PC web privacy policy with mobile apps/mobile web.
- Creating & updating the short-notice, layered privacy policy.

PLEASE DESCRIBE THE HIGH-LEVEL CERTIFICATION STEPS FOR MOBILE

1. Conduct kick-off call
2. Review mobile app, mobile web site and/or PC web site
3. Conduct mobile app and/or site review
4. Issue Mobile Site Findings Report
5. Implement recommended changes
6. Confirm recommended changes
7. Issue certification seal and a link to the short notice privacy policy
8. Incorporate and go live

WHAT DO YOU CHECK FOR DURING THE CERTIFICATION PROCESS?

Our privacy certification process is based on our experience helping thousands of sites, applications and software platforms since 1997.

The certification for mobile apps and mobile websites consists of:

- A review of all key user interactions that are related to the information flow especially those concerning sensitive geo-location data.
- An assessment of data management practices including the collection, storage, use and sharing of personally identifiable data throughout the process.
- Verification of each mobile app, mobile web and/or PC web site against TRUSTe program requirements.

A high level description of our program requirements can be found here http://www.truste.com/privacy_seals_and_services/consumer_privacy/privacy-programs-requirements.html.

HOW IS IMPLEMENTATION DIFFERENT FOR MOBILE APPS VS. MOBILE WEB SITES?

Mobile App - Upon certification approval, you can embed the small mobile seal in key places in your app where you want to assure your users of your privacy practices. The seal should link to the short notice privacy policy if you do not already have a text link to the privacy policy.

DID YOU KNOW?

84% of Consumers Think the TRUSTe Trustmark Is Very/Somewhat Useful in Deciding When and How to Disclose Their Personal Information

- TNS Research, Dec. 2009

If you do not display the seal, you can link to the short notice privacy policy usually through a standalone “privacy” link by placing the link in the “About” “Settings” or “More” section.

Mobile Web - Upon certification approval, you can insert the small mobile seal in key places on your mobile web site where you want to assure your users of your privacy practices. The seal should link to your privacy policy if you do not already have a text link to the short notice privacy policy. If you already have a link to the short notice privacy policy (usually in the footer of the site) then the seal should link to the TRUSTe Validation page.

WHAT TYPE OF CHANGES WILL I HAVE TO MAKE TO MY MOBILE APP IN ORDER TO SHOW TRUSTE CERTIFICATION?

Upon certification approval, most clients simply add a link to the TRUSTe-hosted short notice privacy policy and embed or place the TRUSTe seal on their mobile web site/app.

1. **Certified Privacy seal** -The seal should be linked to the short notice privacy policy if there is no other way for the user to access the privacy policy.
2. **Short Notice, Privacy Policy** - You will need to place a link inside the app or from your mobile web site to a TRUSTe-hosted privacy policy which contains a summary of the key parts that are relevant to your mobile app and/or web. Note that the subsequent pages contain a link to the full privacy policy (hosted on client site); the link is formed by TRUSTe.
3. **Validation page** - A link to the page validating your TRUSTe certification is accessed via the short notice. No action is required on the part of our clients.
4. **Watchdog - Dispute Resolution** flows - A link to this service is located in the body of the validation page and the user is taken to a TRUSTe-hosted dispute resolution flow. No action is required on the part of our client.

TRUSTe has a consultative approach to certification which means that during the review of your mobile web site or mobile app, we will work with you to implement changes that bring you in line with our program requirements. Our approach minimizes any impact to your application development cycle. Most clients are able to simply publish an update to their mobile app by embedding the seal and adding links to the TRUSTe-hosted short notice privacy policy.

HOW DO YOU ENSURE COMPLIANCE THROUGHOUT THE CERTIFICATION TIME PERIOD?

First, we provide users with a link to our Watchdog-Dispute Resolution services through the validation page which allows users to provide feedback (both positive and negative) regarding the mobile app and/or mobile web site they have visited. We use this as an early warning system to make our clients aware of any potential issues.

Next, we perform ongoing reviews during the certification time period anytime we are notified by our clients that their mobile app and/or mobile web site has undergone (or will undergo) a material change*.

Lastly, we randomly select TRUSTe-certified sites and apps for additional in-depth reviews.

*Material Change: Examples include change in scope/type of personally identifiable information collected, addition or modification to major features and functionality, and/or change in data management practices.

WHAT VALUE AM I GETTING IF YOU HAVEN'T CERTIFIED THE APPLE/ ANDROID/BLACKBERRY PLATFORM?

In general, your mobile app or mobile web is reviewed for its practices related to how data is collected, stored, managed and shared regardless of whether the platform is TRUSTe certified. We have deep knowledge of all platform development, legal, technical and privacy requirements as specified by the platform operator's developer program.

Platform certification will make our job easier but does not affect the quality or validity of your certification. All things being equal, users are more likely to download a TRUSTe certified app (you can show the TRUSTe seal in the screen captures of your app on the App store). There is a lot of competition in the app stores so the TRUSTe seal helps differentiate your app from others.

Note: We leverage our close relationship with Apple, Facebook and others to assist those clients that have functionality that requires a unique integration as part of our certification process.

ISN'T CERTIFICATION OF THE SAME APP ACROSS DIFFERENT PLATFORMS THE SAME?

Even if the features and functionality of an app are identical for an Apple, Blackberry and Android app the certification process is a separate endeavor. Each platform has different acceptance criteria and each platform (and sometimes, the OS) causes different features to be programmed differently which can have a material difference in their data management process.

Note: An iPad may be different from an iPhone app even if both are available by Apple. The differences are primarily due to their OS and the features and functionality of the app.

ISN'T CERTIFICATION OF A FREE VS. PAID APP THE SAME?

No. Free apps are typically ad supported and are more complex from a privacy certification POV. We cannot assume that all free apps are a stripped down version of the premium app. Also, our pricing accounts for possible changes/upgrades to features and functionality for the entire duration of the certification time period.

DOES TRUSTE ACCEPT A MOBILE APP (OR MOBILE WEB THAT IS NOT LIVE) THAT IS NOT YET APPROVED BY AN APP STORE?

At this time, we only certify mobile apps that are available publicly as our testing software can only access apps publicly available through an app store. On an exception basis, we can review an app prior to its acceptance. In general, it is difficult to certify if the features and functionality are changing or may change due to app store requirements. It also requires additional work on our part which drives up the cost of certification. We also require that you notify TRUSTe when your app has been accepted or has gone live.

WHAT IF MY APP UNDERGOES A FUNDAMENTAL CHANGE? WHAT ABOUT MINOR UPDATES? DOES THAT MEAN MY CERTIFICATION IS INVALID?

Your privacy certification includes re-certification throughout the duration of your certification time period (typically 1 year or more). Therefore, if your app or mobile web site undergoes a major or minor update after the initial certification and you want your certification to reflect the most recent version, please contact us and provide details of the change.

Please note that you must inform us of material changes as we will not automatically perform a re-certification review.

WHERE CAN I PLACE THE SEAL?

Please see the Mobile Certification seal implementation guidelines. Suggestions for seal placement:

- When you first interact with the app.
- Whenever you are asking for personal information (this is required on key forms, but not all forms) For example, a newsletter subscriptions sign up form may not require a seal or link but a form that requests a user to register would require it.
- Wherever the privacy policy can be accessed such as in the “Settings”, “More” or “About” section of the mobile web site or app; At a minimum, they must have a link to the words “privacy”.
- On screen shots you upload to an app store so users can tell you are TRUSTe certified before they download an app.

Note: You cannot link to the full privacy policy directly or link to the PC web validation page etc.

HOW CAN I MAXIMIZE CONVERSION?

To maximize the benefits of your TRUSTe mobile privacy certification, place the seal near forms that collect personally identifiable or sensitive information (name, email address, age, credit card, password etc.).

You can also place the seal on the app pages that you display in an Apps store to help differentiate your app and maximize the number of downloads. We hope our clients encourage app stores and platforms to prove more integrated displays of trust marks for apps that have undergone third party certification.

Lastly, you should display the TRUSTe seal when your user first interacts with your app.

WHAT TYPE OF APPS ARE NOT ACCEPTED FOR CERTIFICATION BY TRUSTe?

TRUSTe will be unable to certify any app or site that engages in illegal US practices such as child pornography, gambling etc.

Need Help?

To learn more about TRUSTe implementation, best practices or if you have any questions, contact your TRUSTe Client Services Manager.

www.truste.com | twitter.com/truste