

Submitting Organization: TRUSTe
Contact: Rebecca Richards, rrichards@truste.org, 202-483-1900
Paper Name: Considering Choice in the Wireless World
Category: Consent/Choice Options Using Other Media and Devices: wireless, email etc
Format: MS Word
Document Name: Choice Wireless.doc

Considering Choice in the Wireless World

Background

The convergence of wireless technology and mobile computing is creating a new network for consumers to participate in Internet commerce. Current data illustrate the rapidity of this convergence. Consider the following:

- > Today, there are more than 500 million wireless subscribers globally. This is expected to exceed one billion over the next four years.
- > In 1999 more than nine million personal digital assistant (PDA) devices were sold worldwide; this growth is expected to accelerate over the coming years.
- > In the second quarter of 2000, more than half the wireless phones sold were Internet-enabled – this is expected to increase to nearly 70 percent by the end of 2000.

Based on the above, more people are expected to access the Internet via mobile devices than through PCs in the next four to five years. If these metrics are a leading indicator of mass consumer adoption, then the Wireless Internet will become the second Internet Revolution.

However, just as the emergence of networked databases in the Internet economy have placed greater emphasis on consumer privacy protection, so too will the burgeoning Wireless Internet lead to important privacy considerations. As such, government, industry and consumer groups have the unique opportunity to understand and address the issues surrounding protection of personal information that will shape this new medium.

Factors Impacting Privacy in the Wireless World

While data protection is not new to mobile commerce, there are privacy-related issues that are unique to the wireless world. TRUSTe has identified several issues that should be considered when determining how to provide individuals with control over their personal information and providing them with choice in the protection of personally identifiable information in the wireless world. Some of the issues include:

Privacy Policies –

Privacy Statements -- Small screen sizes on mobile devices coupled with relatively slow transmission speeds impact a user's ability to read and understand effectively a privacy statement. Lengthy, multi-page disclosures will lose their effectiveness in providing privacy protection. As more consumers embrace the wireless Internet – and more companies embrace it as a means to communicate to their customers – industry must consider alternative and complementary methods to communicate privacy policies to consumers. Some primary questions include:

- > How should a consumer be notified about privacy practices?
- > What is a reasonable burden to put on companies and what should be expected of consumers to protect their privacy?
- > Are written statements and seal certification programs sufficient?
- > What technological solutions will help balance the need for adequate communication of privacy policies?

Technology Considerations – New technology will help streamline the process of privacy disclosure by giving users the ability to set automated privacy preferences. These technologies should be rooted into the architecture of the wireless web, namely the Wireless Application Protocol (WAP). Stakeholders in enhancing privacy protection in the wireless medium should call on the World Wide Web Consortium (W3C) to assess its ability to port P3P-related technology to mobile and wireless devices. Similar to its use through browsers, P3P should allow users to set preferences that, for example, only transmit data to companies that are endorsed by third party oversight programs or that adhere to certain privacy standards.

Seal Programs – Thus far, seal programs such as TRUSTe have been critical to building an architecture of trust online by using a visual symbol to indicate to consumers that a Web site has undergone comprehensive certification. In essence, these seals have been important visual guideposts to sites that can be trusted – conversely, the absence of such seals indicate that perhaps a site should not be trusted with personal information.

Enforcement programs that offer visual guideposts (i.e. seals) will continue to be critical in helping consumers easily and effectively understand a company's privacy practices. In the Wireless World, privacy seals become even more critical for consumers given the difficulty of reading privacy statements on the small screens of mobile devices.

The greater importance of seal programs in the wireless world, however, raises significant questions that must be considered. For example, if a seal program sets specific standards that all holders must abide by, how does this differ from government regulation? Will the policies of seal programs be sufficiently flexible

to accommodate different business practices and legislation for mandatory emergency tracking while balancing the privacy rights of individuals?

It is reasonable to assume that the same market forces that have led businesses to adopt ethical privacy practices will also take hold in the wireless arena. If seal programs emerge as a guidepost to trusted commerce sites, how will consumers be educated about different standards? Are the seal programs in essence creating standards and is this good or bad? How will the standards of a seal program be affected by any international requirements?

Opt-in versus Opt-out – The power to control the uses of personal information depends, in part, on a user's ability to prevent tracking and sharing of data. Traditionally, opt-out mechanisms that give people choice are adequate to fulfill this requirement. If GPS technology is used to its fullest extent, however, then tracking can occur before consumers are given the ability to choose. We must consider whether consumer protection of their personal data in the Wireless World requires an Opt-In approach.

We must also consider whether there are legitimate business models that make Opt-Out appropriate. How would a blanket mandate for Opt-In impact the growth of this new industry?

Other Considerations

Security -- Given the inherent insecurity of transmitting data in a wireless world, what are the measures of reasonable security?

International Considerations – The Internet is by nature global. How will the decisions we make in the U.S. affect or be affected by international decisions of international organizations and other national governments? How will jurisdiction be dictated?

Responsibilities – Which parties bear the responsibilities of protecting personal information? Is it the manufacturer of the wireless device, the wireless supplier, or the content service?