BIZCOMMUNITY

Mobile privacy 2012: where in the world is your data?

By Wikus Engelbrecht

28 Mar 2012

Mobile tools and applications represent a powerful technology that will most certainly become more important in years to come. Gartner Research has predicted that, by 2013, a greater number of people will be accessing the internet via mobile devices than those who will via desktop computers.

More aware of being tracked

With this move towards the small screen, consumers are becoming more aware of being tracked through mobile connectivity. The unique characteristics of the smartphone as a platform that's always on, connected and providing access to real-world information such as user location, habits, schedule and lifestyle are creating a number of privacy challenges.

Given the sensitivity of the data that many consumers store on their phones, the demands are very high for manufacturers, marketers, carriers, app developers, ad networks and all other mobile service providers to respect user privacy in order to earn and retain public trust.

Making sure users feel that they are in control of sharing their data is important. After all, companies can't afford for consumers to perceive a lack of control over a device that is so intimate.

Considering how sophisticated mobile data has become, and how widely this data is being leveraged for business and commercial purposes, 2012 will be a critical period as the industry will face growing scrutiny around privacy concerns from the media, regulators and governments.

Mobile privacy and the long arm of the law

Practices surrounding the disclosure of consumer data do not appear to have kept pace with the rapid developments in technology. Referencing a Future of Privacy Forum study from December 2011, the NTIA (National Telecommunications and Information Administration) has stated that only about 30% of the top 10 paid mobile apps for three major mobile operating systems have legitimate privacy policies.

One can then only imagine how leaky the privacy hull within the free mobile app environment really is.

With the abundance of unregulated data available out there, and with many terabytes more of it being generated daily, phishers, spammers and data-ravenous marketers have been having a picnic.

And so this year, the industry is expecting to see a large amount of legal action around mobile privacy on a couple of fronts that are danger areas where data-users are running afoul of consumers; mainly including location-based data and stricter privacy policies for mobile use by children.

Clash directly

Of these two, location-based services in particular have become a huge trend in mobile and have been an important part of the global discussion, as the need for geo-based information to provide certain mobile services clashes very directly with desire and need for privacy.

For the time being, there is not yet a good set of universal rules for what can and can't be done with location-centered data to make advertising more effective, and this is precisely where companies overzealous about using this info are going to invite controversy.

How location data is being shared is something that still needs to be fully resolved.

To begin with, business owners looking to keep from straying into regulatory cracks and grey areas should not sell or trade away this information, so that other companies can flesh-out a profile of where a user has been, what they have bought and why, over time.

Framework taking shape

Fortunately, a framework for understanding the privacy rights needs of mobile users is busy taking shape.

In February 2012, talks at the Mobile World Congress in Spain highlighted the work being done by various sectors on addressing the challenges of mobile privacy, including the GSMA's own initiatives.

Now, the GSMA, with the support of leading mobile operators in Europe and following consultation across the wider mobile ecosystem, has published a set of global Privacy Design Guidelines for Mobile Application Development. These new guidelines aim to provide users with better transparency, choice and control over how apps use their personal information.

The privacy guidelines, which are being implemented currently by a number of mobile operators in Europe for their own branded applications, are an important first step.

Real change needs close, lasting collaboration

To effect real change, there will need to be close and lasting collaboration between industry giants and governments.

Policymakers in Washington DC, USA are currently on the edge of their seats, anticipating the release of two major mobile-oriented privacy documents within the next few months.

It's expected that the White House will endorse a privacy model that would see leaders in the mobile arena come up with self-regulation procedures, after which the Federal Trade Commission will determine the adequacy of the new rules (or not), and then decide whether to approve and enforce them as if they were law.

An obvious, but key challenge is how to give users simple, device and context-appropriate ways to manage their own data.

Service providers taking the initiative

Despite delays in establishing a ubiquitous, systemised framework for breeding privacy measures into the hand-held setting, some service providers have started taking their own initiatives towards data control.

Mozilla, for example, was the first major browser to provide its users with 'Do Not Track' (DNT) features on both desktop and mobile. Firefox for Android provides users with the ability to send the DNT header to websites visited via the browser, as well as to any third parties trawling for information.

As of 26 February 2012, 18% of users of Firefox for Android had turned on DNT, but even if all the other native browsers on mobile followed their lead, there's still an opportunity for applications installed in mobile devices that include services from third parties, such as retailers and social media platforms, to bypass the DNT header.

In order to maintain strong growth in both the sales and popularity of mobile apps, customers need to be confident that their privacy is protected when they use them. This is the responsibility of the entire mobile industry.

Interdependent concepts

In the long run, it seems unlikely that people will tolerate a device that is in their pocket as being anything less than something they are in complete control of. Thus, industry players must view mobility and privacy as interdependent concepts and do what they can to respect user privacy.

ABOUT WIKUS ENGELBRECHT

Wikus Engelbrecht is a marketing writer, journalist and media liaison at GraphicMail (www.graphicmail.co.za; @GraphicMail), an international email and mobile marketing service provider. Since 2003, his professional career in language and media has spanned the film, print advertising, magazine publishing, web development and online content industries. Contact Wikus at wikus@graphicmail.com and follow @WKS_Engelbrecht on Twitter.

- QR codes bring email, mobile coupons to life - 31 Jul 2012
- The role of email marketing in the multi-channel evolution: Part 4 - 4 Jul 2012
- The role of email marketing in the multi-channel evolution: Part 3 - 27 Jun 2012
- The role of email marketing in the multi-channel evolution: Part 2 - 25 Jun 2012
- The role of email marketing in the multi-channel evolution: Part 1 - 21 Jun 2012

View my profile and articles...