Datamation

7 Hot Mobile Trends for 2012

By Jeff Vance
December 14, 2011

2011 was a crazy year for mobile technology. iPads took the world by storm. Smartphones steadily replaced (and are starting to displace) feature phones. Carrier IQ put us all on notice that mobile privacy could be a major problem in the coming years. RIM finally opened up BES to other mobile OSes, which is pretty much the only move it had left to stave off extinction.

If 2011 was a tumultuous year, 2012 is shaping up to be even more chaotic. The inevitable invasion of smartphones and tablets into the enterprise will have CIOs scrambling to figure out BYOD solutions. Microsoft will finally start to challenge Apple and Android, and new types of mobile apps will start to emerge, such as context-aware apps and mobile wallets.

Here are 7 mobile trends to watch for in 2012:

1. Privacy continues to erode

Privacy took a beating in 2011, and 2012 could be even worse. Smartphones and social media are two of the main culprits eroding our privacy. Facebook has taken a beating, although Facebook's settlement with the FTC should help.

Smartphones, though, represent a bigger privacy threat than social media. Yes, phishing attacks increasingly rely on social media, but information about you on social media is more or less information you decided to put there. There are exceptions (i.e., someone tagging you in a picture), but for the most part, the easiest way to keep sensitive information off social networks is to not put it there in the first place.

Smartphones present a more vexing privacy conundrum. Pretty much every app you download asks for all sorts of permissions, and most of us blindly hit "accept." If you want the app, you really don't have a choice. GPS tracking can pinpoint your every move, and even when companies say they aren't keeping information about you, you'd be a fool to trust them.

Case in point: Carrier IQ's apparent invasion of privacy. The company's software is supposed to perform diagnostic tests to improve the user experience, but the software itself does many of the same things malware does, including keylogging. (Carrier IQ disputes this.)

The software has logged SMS messages, kept track of phone calls and web browsing history and tracked locations. All the major mobile players are scrambling to distance themselves from Carrier IQ, but where was all of this consternation before the story broke? Why did they let software like this onto smartphones in the first place? Because they want to know everything they can about you. It helps them sell you stuff (and less ominously, much of this data can be used to improve the user experience).