



Steve Montgomery



The Internet of Things Must Be Safe & Easy



Steve Montgomery, General Manager, Digital Six Laboratories, LLC,
11/6/2013

[Bio](#) [Email This](#) [Print](#) [Comment](#) [2 comments](#)

[Login](#)

 
50% 50%

No one can deny that the Internet has had a profound impact on society as a whole. It is a rare person whose normal day is not touched by e-commerce, social media, or search engines. The Internet of Things (IoT) promises to make an even more profound impact because of its automatic nature. As developers, we have a duty to make sure that impact is beneficial.

I was happy when Rich Quinnell invited me to blog on this site. I absolutely live, eat, and breathe the IoT right now, and I love almost every aspect of it. But what is the IoT, exactly?

Whenever I get on to a new topic, I usually like to start with a definition, but we cannot in this case. [Kevin Ashton](#), who proposed the term in 1999, said the IoT is more of a concept than anything else, and therefore it is really not possible to make an official definition. Instead, I will attempt to define it by example.

Over most of the past 13 years, my experience with the IoT was limited to commercial and industrial applications. I developed a complete monitoring system for oil and gas wells that grabs local data from the well site automation system and forwards it to a central server via the Internet. Traditionally, that is what the primary development effort has looked like in the IoT space. Today, however, there is a very exciting paradigm emerging within the IoT space that I call lifestyle automation. Whereas a commercial IoT application might be monitoring an oil well using the Internet, a lifestyle automation application might make your trashcan tweet a message when your dog knocks it over.

That might seem like a farfetched application to you, but I assure you that it is closer to reality than you think. In fact, it is an application close to my heart. I am weary of my wife complaining about my dog getting into the bathroom trash. If I could get a notification (and tweeting is an easy, cheap way to get it), I could clean up the mess before she found it. That would improve my life more than I can put into words.

The cool thing is that this type of application is actually possible to create. In fact, my company, Digital Six Technologies, is working on an open-source platform called Angel Blocks (which will soon be launched on [KickStarter](#)) that aims to make exactly this kind of thing possible. But there are some concerns.

As we were developing our approach, I talked to a bunch of people I know who are generally early adopters and risk takers. I wanted to know what they thought of our technology. One recurring theme in the feedback that really shocked me was fear about privacy and security. In almost every case, the first and greatest concern was "If I use a cloud-based application to

control the things I connect together via the Internet, how I can be sure that no one can gain control of my things and either learn information about my life or control aspects of my life?"

That is a very good question. Recent stories about the [IRS](#) and [NSA](#) make nearly all Americans -- and hopefully all citizens of the free world -- more sensitive to their personal privacy. Many are becoming more deliberate about how they expose that data to the cloud, where hackers, criminals, and even snooping governments can get at it.

For this reason, I think that we, as IoT developers, must at least begin a dialogue about the ramifications of connecting nearly every aspect of a person's daily life to the cloud. An amazing amount of information can be inferred from the kind of data that can be collected by a personal IoT application. We need to consider what that means to the products we are developing.

Personal IoT applications not only collect data, but they can also provide control. That is an even greater threat, in my mind. A simple virus called Stuxnet shut down Iran's nuclear fuel processing facilities. If Iran could not protect its nuclear system automation, what chances have average consumers of protecting their IoT devices? We must seriously consider the implications of putting our personal lifestyle automation applications online via the IoT.

We are struggling with this issue as we develop our Angel Blocks platform. It is an IoT solution for makers, so our problem is a bit easier. We are working with technically savvy users who can tolerate a more complicated configuration process, including setting firewall rules. Our gateway, the Angel Gate, is also the primary database server and resides at the local site. For absolute security, the user can put the Angel Gate behind a firewall and VPN in, though that is not required. The user can use technologies like Twitter and Facebook to publish some data and email/SMS to keep some data private. Really sensitive data can be viewed locally with a smartphone, tablet, or PC.

For makers, I think that such a compromise of increased complexity for added security is valid, but it might not be valid for general consumers. The beauty of the cloud is that it can make the customer's setup and use experience flawless and seamless, requiring no technical knowledge. We need to preserve that simplicity in our product designs.

The question in my mind is how to provide an easy-to-use system to general consumers without exposing them to the privacy dangers of the cloud. I am very curious to know what you think about it.

[Email This](#) [Print](#) [Comment](#)

Copyright © 2013 TechWeb, A UBM Company, All rights reserved.