I COULD MAKE a strong argument, I think, that mobile computing has been one of the most transformative recent technologies to impact our daily lives. Thanks to mobile devices, we all have instant access to the voices of our loved ones, maps, navigational info, on-demand movies and games, even our extensive music collections. We’re wired together and can keep tabs on each other at almost every moment of the day.

In this issue, we feature several articles that focus on the technical breakthroughs that have allowed this revolution to happen and that are enabling even more sophisticated behaviors.

But it would be remiss to focus on this topic without discussing privacy, one of the most troubling issues surrounding our increasing dependence on mobile computing.

I suspect that many users feel barraged with requests from installed apps that continually want access to various bits of personal information. (At least I do.) Not that mobile computing is inherently dangerous, but many apps can use personal information in ways that aren’t palatable and are often misunderstood. The recent story about the flashlight app for Android phones, which, once installed, automatically collected information about its users and shared them with third-party advertisers (www.businessinsider.com/android-flashlight-app-privacy-flaw-2013-12), is a cautionary tale about the potential for abuse that exists in even seemingly innocuous apps.

To get a handle on privacy risks and better calibrate how much we should worry about such things, I spoke with John Howie, chief operating officer at the Cloud Security Alliance, a not-for-profit organization that focuses on education and best practices for providing security assurance within cloud computing. In addition to outlining privacy issues with which mobile users should be familiar, he also articulated important lessons about developers’ roles and responsibilities where privacy is concerned.

FS: I tend to look at mobility as a tradeoff between convenience on the one hand and privacy on the other. There are some tradeoffs I’m willing to make—I find it very convenient to have GPS navigation when driving to an unfamiliar place, even if it means I might be making my location information available—and then there are others where the price is too high for the benefit that I get. Is it fair to think of privacy and convenience as two opposite ends of a scale?

JH: This is a very nuanced question with an even more nuanced answer,
unfortunately. It really depends on the device and the application that you’re using and how you’re using it. There is certainly cause for concern among many professionals, both of privacy and classic information security, about the inadvertent use of a mobile device to access business information from a secure cloud that inadvertently leaks and is lost to the control of the organization.

Here’s a great example: Let’s say that you’ve got a cloud-based email service and you’re using a mobile device, say a smartphone. You open up an attachment to an email that contains sensitive information, say a customer list. You hit save on that attachment once you’ve opened and read it on your device—and without your knowledge, that file has now been backed up to the cloud service that backs up your mobile phone. (In the case of a Windows phone, it’s SkyDrive; in the case of an Android, it’s Google Drive; and in the case of an iPhone, it’s iCloud.) You’ve now inadvertently taken very sensitive corporate information and made it available in your private, personal cloud storage, and the organization has essentially lost control of it. There’s actually a case to be made that in such situations, the organization must do a breach disclosure under the various state laws that exist in the US and the various national laws that exist in other countries overseas. So yes, there is definitely a privacy concern at the intersection of mobile and cloud technologies.

Going beyond that, we see mobile devices becoming ever more powerful and including an array of sensors—such as location, environmental, and Bluetooth and RFID—allowing information to be unwittingly collected by your device, consumed by an application, and then stored in the cloud. So, personal privacy is being threatened as well.

FS: As the number of sensors and opportunities for automated data collection on wearable devices increase, will the problem only get worse? Or are there trends that make you more optimistic that privacy issues can come back under the control of the individual person?

JH: That’s a difficult question to answer. I’d have to start by giving my view of what’s going to happen in the future, just to put my answer into context.

I think in the next five years, you’re definitely going to see your phone continue to be a hub of sorts, on and around your body. So things like your Fitbits, Nike FuelBands, or Google Glass are going to communicate with your mobile device. And your mobile device is going to be the gateway to the cloud. You’re going to have a personal area network around you of devices that communicate with your phone or your tablet. What you have to be aware of is that over the next five years, these devices are going to become ever more powerful, with more storage and processing options. As a consequence, a lot more of the data crunching required in big data scenarios can actually now happen on the mobile endpoint or on the device itself. Then, the distilled information will be uploaded into a cloud service, where it’s then collocated with other information (yours and other people’s), and then that aggregate will be analyzed and crunched to derive ever more useful information.

The question that needs to be addressed is, at what point does the consumer have control over the collection and the analysis of the information, either on the device or in the cloud? And how can he or she specify its allowable use?

One thing that I don’t think individuals truly understand is the business model that comes with free applications. Remember from your high school economics class that nothing is free! We use these free tools, and in return we have to sacrifice something, a little bit of our privacy. Why? The companies that provide these free tools live off ad-
generated revenue. When we download applications that offer to monitor our health for us or provide suggestions for a healthier lifestyle or tell us about special offers, they’re using information that we voluntarily give them, either explicitly by having us input profiles and select preferences or implicitly by having the device sense where we are and what we’re doing. Consumers need to understand that they’re getting a service, and in return they have to sacrifice a bit of their privacy.

It really behooves the developers and the industry in general to educate consumers and users about privacy choices and what they’re going to be giving up in return for a service. That’s going to require software developers to understand how to build privacy controls into applications so that I may, as an informed consumer, download an application and know what I’m going to have to give up, which might be location information, lifestyle information, or demographic information. And I have to be willing to say, well, I’m willing to share this and I’ll get that in return, but I’m not willing to share this other piece of information, and that means I’m not going to receive these benefits. Developers are going to have to understand how to build that kind of privacy choice based on notice, choice, and consent, which are the principles of privacy, into the applications that are on our devices.

Developers can’t just simply build an application that invades people’s privacy even though it’s “free.” Developers have to make the notice available and allow users to make a choice and give informed consent.

**FS:** So one of the jobs that developers need training and education in is how to give users a much more fine-grained choice about what types of personal information they are willing to share?

**JH:** That’s correct. But it can’t just be a toggle switch. People have to understand what they’re giving up and what they’re getting in return. The developers need to enable these privacy tradeoffs in the application. But an analyst or a privacy expert is going to have to craft the notice, choice, and consent that comes around the application so that the developers can understand that and programmatically build it into the app.

**FS:** Are you aware of any work that’s intended to help developers have that dialog with users to help them understand these privacy tradeoffs? Is there a risk that as more developers try to provide these options, we get to a situation where the user becomes overwhelmed by choices from the applications he or she wants to use? Being constantly barraged with requests may be just as bad as having too few options.

**JH:** There is an industry nonprofit organizations that the Cloud Security Alliance works very closely with called the International Association of Privacy Professionals. Their website (www.privacyassociation.org) provides a wealth of resources to their members that raise awareness of privacy and help organizations build privacy programs. If you’re a developer, they’ve got a certification program, which helps educate developers and IT folks about some of the issues that come into play when handling user information.

But companies that might surprise you, such as Microsoft, have...
actually spent a lot of time looking at this as well. Given that Microsoft works in the mobile domain and has in the past been accused of privacy violations, they’ve taken privacy to heart. Microsoft is better known for its security development lifecycle (SDL), which is how Microsoft writes software to ensure that it meets trustworthy computing principles. Their Microsoft Privacy Standards for Development, which was originally a separate document, is now written directly into the SDL. The SDL is freely available; you can go to the Microsoft website (www.microsoft.com/sdl) and download all their resources to see how Microsoft has built privacy into software development at each key point.

The SDL is a series of development guidelines that should be considered when building software. It doesn’t really help organizations consider the privacy tradeoffs in the first place. For that, you’re going to need to build a team of privacy experts who can look at what your business goals are and what’s required to achieve those business goals in terms of the personal identifiable information from a device or application user. You’ll need to build a series of controls around how that information is collected, disseminated, and used within your organization and with your partner organizations. You’ll need to formulate how to communicate that to consumers, allow them to make their choice, and provide their informed consent.

FS: This sounds like it requires a lot of training and a lot of different kinds of expertise within a company to do it right. What kind of advice can you give for developers at small organizations who might find this daunting but who want to do it right?

JH: Small companies are always going to struggle with this. The people who can make an impact are the ones at medium and large companies, the ones that have become a bit more stable and sensible and are looking at new revenue opportunities; perhaps they’re able to offer paid-for applications that don’t rely on ad-generated revenue.

You actually see this in some of the large email providers, Microsoft, for example (and Google does the same): you can actually buy from them the ability not to be served advertisements. You can go to your online email and not have adverts because Microsoft or Google will take a small subscription fee from you instead. That’s another tradeoff: Do you want to start paying for applications?

So there are things that developers can do, but there are also things that consumers need to be more savvy about. As consumers, we need to be able to say to our content or application providers, “Look, great application, great idea … but I’m never going to use it, because you’re going to consume this personal information about me. How about I pay you a small monthly amount of money? Will that meet your needs instead?” Once companies see that their customers are willing to pay that amount of money for a professional version of the apps and they don’t have to rely on ad-generated revenue, we might see a shift in the industry toward a model that’s more privacy-aware.

SOFTWARE EXPERTS SUMMIT 2014: SAVE THE DATE!

One of my goals as editor in chief has been to publicize IEEE Software in geographic regions where we aren’t as well represented. I’m excited to report that Software Experts Summit (SES) 2014 will be held in Bangalore, India, on Friday, 30 May.

SES is a public event that showcases many of the thought leaders associated with the magazine during a day of presentations, panel discussions, and networking. Our theme this year is “Software Engineering for the 21st Century,” and we’ll be featuring a variety of speakers to cover the latest important technologies that are transforming our field. Our goal is to provide attendees with the information and resources to ride the wave of the latest changes in software engineering and keep up to date with the tools they need as practicing software engineers.

We’ve already lined up exciting speakers including Jan Bosch, Michiel van Genuchten, and Tom Zimmermann. And we extend many thanks to our general chair for the event, Girish Suryanarayana of Siemens.

For more information, check our website at www.computer.org/ses14 (which we’ll keep updating as new details are nailed down) and the ad on page 1 of this issue.
FS: So we’ve talked about strategies for both developers and users, to help improve issues related to privacy for mobile and cloud software. Anything else we should keep in mind?

JH: Users have to be aware of what they are getting into. It really is *caveat emptor*, “buyer beware.” Yes, you’re not paying anything, but you’re not getting it for free. Until consumers at least understand what they’re giving up in return for “free” apps, there will be a problem. The downside of this is what will happen if consumers don’t start making more intelligent decisions for themselves and if the industry doesn’t step up and clearly spell out what it’s collecting, how it’s collected, and what it’s used for. In this case, you’re going to see legislators step in and start passing some laws that, as an industry, we don’t want to see. Self-regulation is always better than legislation.

As an industry, we have to be very cognizant of both the power and the benefits that cloud and mobile computing can bring to society. There are some wonderful opportunities here to dramatically improve people’s lives, especially around health, welfare, and fitness. But it can also be a bane to the existence of many when we start to invade people’s privacy. So there will be tradeoffs, and we have to make informed, intelligent tradeoffs both at the developer and consumer levels. Everyone has to come together to have the debate about what is right, good, bad, wrong, or creepy. Then, as a society, we can have a consensus.

FORREST SHULL is assistant director for empirical research in the Software Solutions Division of the Software Engineering Institute, a federally funded research and development center based at Carnegie Mellon University. He is editor in chief of *IEEE Software*. Contact him at fshull@computer.org.

SOFTWARE ENGINEERING RADIO’S 200TH EPISODE

In my mind, one of the most exciting resources associated with *IEEE Software* is our monthly Software Engineering Radio (SE Radio) podcast. SE Radio was founded in January 2006 by Markus Voelter. It joined forces with *IEEE Software* in February 2012 and reaches about 40,000 listeners with each episode.

SE Radio is targeted at the professional software developer. The goal is to be a lasting educational resource, not a newscast. Episodes are either tutorials on specific topics or interviews with well-known experts from the software engineering world.

I’m very pleased that we’ve just posted the 200th episode, an important milestone that shows the dedication of the creative team of volunteers as well as the huge interest in these topics. To commemorate the event, we’ve invited Markus Voelter back. This time, he’s on the other side of the microphone as an interviewee talking about his very exciting work in the area of domain-specific languages.

Interested? Browse our past episodes. Whatever your interests in software engineering, I’m sure you’ll find episodes that are right up your alley. (One of my personal favorites is from 2008 with Linda Rising talking about retrospectives: www.se-radio.net/episode-105-retrospectives-with-linda-rising.) You can find us on iTunes or at www.se-radio.net. (And for our loyal listeners, please note that we’re further celebrating this milestone with an elegant redesign of the website. Enjoy!)

Division of the Software Engineering Institute, a federally funded research and development center based at Carnegie Mellon University. He is editor in chief of *IEEE Software*. Contact him at fshull@computer.org.

See www.computer.org/software-multimedia for multimedia content related to this article.

NEXT ISSUE:

May/June 2014

Green Software