As a computer scientist, I feel like I’ve been remarkably behind the curve in the mobile phone department, having put up with mobile “dumb phones” for more than 15 years before recently getting my first “smart phone.” Now, I can finally hold my head high when I go to a conference or other business meeting, instead of sneaking peeks at my old, unfashionable, and fairly useless phone under the table.

Although I’d done some research on mobile computing many years ago, and was even one of the early users of the ill-fated Eo tablet/phone system (http://en.wikipedia.org/wiki/Eo_Personal_Communicator) – very much ahead of its time – I really hadn’t paid much attention to the applications available for smart phone users in their respective “applications stores” until I had a phone of my own. My experience, along with several recent articles in the popular press, have really opened my eyes — with rather a deer-in-the-headlights expression, I fear. On one hand, the applications I run want to do all sorts of things to my phone; on the other, the carriers are trying to figure out how to keep these applications from overrunning their networks.

Location, Location, Location
Any IC reader likely knows that location-based services are important and have evolved from an interesting research topic to a real-world ecosystem. Applications range from navigation (routings, finding local businesses) to commerce (coupons, paying your dinner bill over your mobile phone) to peace of mind (Where the heck’s my phone? Where the heck’s my kid?).

Some applications, such as navigation, obviously require that location information be exposed to the application and perhaps, by extension, to the service provider. Some applications are less obvious about the fact that they require access to various information. When I install a new application and my phone confirms that I’m willing to grant it access to certain information, I try to think long and hard before approving something that combines knowledge about me and my location with access to the network. I find the set of applications (such as Foursquare) that encourage people to semi-publicly post their location to be really curious. After hearing about someone who was friended by an old high school acquaintance on Facebook and then reportedly robbed by that person after announcing plans to attend a concert, I’m not sure what I can say to anyone. (No offense to my 700 friends intended.)

Location-based “games” to get discounts are an interesting change in this space. The New York Times reported that a company called Loopt is turning the mobile phone into a loyalty card by having you “check in” at a location such as a coffee shop to earn points (see www.nytimes.com/2010/06/01/technology/01loopt.html):

Gap is sending customers a 25-percent discount coupon after they check in twice to a Gap store. Burger King is offering a soda with a sandwich or a coffee with a breakfast sandwich to people who check in three times. Universal Music will send five free songs to people who check into any bar along with two friends.

I use my registered Starbucks card far too...
often, and I earn a free drink after every 15th purchase. But my purchases are between me and Starbucks. Another quote in the Times article doesn’t sit well with me: “People register for Loopt Star using their Facebook log-ins, so they can share their location and compete in the game with their Facebook friends and alert their friends about recent purchases and special deals.” I might use my phone in place of a card/key tag to get this sort of benefit at various stores, but I certainly don’t want to post each one to a social network.

Trust but Verify?

One of the interesting apps my wife found shortly after obtaining her Droid is a company called Lookout (www.mylookout.com). It offers a trifecta of security, backup, and location information. For network activity and application issues, any extra security seems like a good thing, though my mobile security friends say you need a completely different security model from the beginning. I would think that a mobile carrier would offer secure application backup just like they currently do for contact lists, but, assuming mine doesn’t, this seems useful. And for location, Lookout offers both the ability to locate a registered phone and to make it sound an alarm on demand.

What’s there not to like? Well, personally, I’m torn. I think the antivirus and firewall are no-brainers. I think the location availability is, in general, very nice, but it does add a vulnerability: anyone I tell where I am can potentially be like that high school classmate I mentioned and use that information for other purposes (privacy policies notwithstanding). Even historical information could be saved (by a company such as Lookout or by the mobile carrier) and used later. Finally, if I put personal data on my phone, and this data gets backed up, it exposes that information to a potential “bad apple,” and I won’t even know it’s been exposed.

The same is true in nonmobile environments, of course. There are online backup providers that will let home or small office users copy their data into servers. Typically, they let the user specify what to back up and whether to encrypt the data, which is more control than I believe I’m offered on my phone. But I would only let such an application onto my computer in the first place if it comes from a company I trust.

All You Can Eat

All these applications create a high demand for the mobile network, so I’ll end with a reference to the recent announcement by AT&T that new smartphone customers would be offered a pay-as-you-go data plan rather than the current unlimited plan. They’re moving from US$30 for unlimited usage to $15 for 250 Mbytes/month and $25 for 2 Gbytes/month, each with additional costs for exceeding the limits, but they’re keeping the $30 plan for existing users who choose not to downgrade. What to do?

I have two unlimited plans with Verizon Wireless for my Droids, and while I’m not happy about spending $30/month for each phone, I’m also glad that I don’t have to worry about usage, at least for now. I also have a USB-based wireless modem for my laptop — until the contract ends in a few weeks — which costs $60/month for up to 5 Gbytes of data.

For the wireless modem, I had a choice between a $40/month plan that was limited to 250 Mbytes and the $60/month plan with a much higher limit, and I opted for the latter. I didn’t want to nickel and dime myself or worry about suddenly being hit with a $100+ bill. But, in practice, I’ve rarely, if ever, exceeded the 250-Mbyte threshold, and my laptop usage is very much in keeping with AT&T’s claim that most of its mobile phone users fall below this threshold and would save significantly by dropping to $15/month. Even so, my gut reaction was that, if Verizon Wireless offered the
same tiers and, like AT&T, grandfathered me as an existing customer to keep the unlimited plan for $30, I would want to maintain the status quo. I don’t have enough experience with the mobile phone to have any idea what my 3G usage will look like over the next few years. I do know that I expect to use applications such as Pandora that consume bandwidth in ways I never bothered with on my laptop, but I’m not sure yet how much of that usage will be over 3G (where it would be metered) rather than Wi-Fi.

But this isn’t clear-cut. The New York Times columnist David Pogue blogged about how AT&T had done most users a favor while expanding its own customer base by reaching its own customer base by reaching out to people who wouldn’t commit to the current $30/month plan (http://pogue.blogs.nytimes.com/2010/06/03/atts-capped-data-plan-could-save-you-money), ending with an interesting quote:

Maybe I’m just dazzled by the $360 a year AT&T just saved me. But as I see it, AT&T has just pulled off a very delicate balancing act indeed: it came up with a new pricing scheme that benefits almost everyone, customers and AT&T alike.

Barry Leiba, a member of IC’s editorial board, made a similar argument in his blog (staringatemptypages.blogspot.com/2010/06/all-you-can-eat-data.html). With respect to the discussion of $25 for 2 Gbytes/month compared to $30 for unlimited usage, he raised the interesting point that, if you assume you’ll almost always fit within 2 Gbytes, you can easily afford the $10 penalty for exceeding it once in a while.

In the end, I can’t fault carriers for moving away from all-you-can-eat pricing. It was clear from the introduction of the iPhone on AT&T’s network and the complaints about network performance that wireless bandwidth isn’t free for the taking. Carriers must discourage users from “abusing” the network, either by increasing the marginal costs or by degrading their performance relative to the conformers. And those in the US will just have to start living like the rest of the world.

Acknowledgments

The opinions expressed in this column are my personal opinions. I speak neither for my employer nor for IEEE Internet Computing in this regard, and any errors or omissions are my own. Thanks to Lisa Bahler, Robin Chen, Kris Hildrum, and Barry Leiba for their helpful comments.

In the end, I can’t fault carriers for moving away from all-you-can-eat pricing. It was clear from the introduction of the iPhone on AT&T’s network and the complaints about network performance that wireless bandwidth isn’t free for the taking. Carriers must discourage users from “abusing” the network, either by increasing the marginal costs or by degrading their performance relative to the conformers. And those in the US will just have to start living like the rest of the world.