There is a kind of beguiling attraction to putting appliances up on the Internet for local and possible remote interaction. Managing entertainment appliances remotely (even contracting to have entertainment recorded per your instructions by third parties) sounds so convenient. Similarly, monitoring sensor networks, including security and environmental sensors, sounds like an obvious application. The idea of being able to (sort of) log into an appliance to configure it using a simple browser has its appeal. Many systems support such applications today. Some of them have already surfaced as applications running on mobile devices. How convenient to turn up the heat remotely before you get home on a cold winter day. I have been thinking a lot about this lately — and I am worried.

A brief digression (well, ok, rant). I have a few printers around the house. Laptops come and go here with some frequency. I’ve noted increasing difficulty getting printer drivers for different versions of operating systems on various platforms. In fact, configuring various brands and vintages of printers, laptops, and other computing devices to work with the printers has been rather difficult. On the presumption that I’m not the only person with this problem, it seems worth trying to understand what’s going on.

It’s clear that others have recognized this problem and tried to do something about it. “Cloud printing” is one example. In the Google version of this (http://support.google.com/cloudprint), either the printer is itself capable of Web-based interactions, or it’s connected to a computer that has a conventional printer driver and also is connected to the Internet and can respond to “cloud print” requests. Access control is an important matter — we don’t want junk print jobs any more than we wanted spam fax messages to consume our resources. When you enable a printer to be “cloud ready,” you can also determine who has access to the printer by associating a person’s Google account with access to the Web-enabled or classic printer. This kind of solution means that the print job’s originator doesn’t need printer driver software for the target printer. From my viewpoint, this is a primary value of this design. Another is the ability to print remotely — a kind of modern fax service.

This column’s focus is more on the problem of configuration and access control for a multitude of network-enabled devices. If we really look forward to having many appliances and devices online, but we care who has access to them remotely and what they can do with that access, then we’re going to have to ask how configuration and access control can be made as simple as possible. What will happen after a power failure? How hard will it be to reconfigure everything if you move to a new location? These aren’t idle questions, and finding ways to make the process simple while preserving access control and privacy is a nontrivial design challenge. Many readers will be familiar with the Blue Tooth mechanism for linking two devices to each other. It’s a fairly simple procedure but relies on the two devices’ proximity. In the case of devices that need to be associated remotely (and might never be in physical proximity), alternative methods are needed. A distinction also exists between giving yourself remote access to a device or appliance and giving access to a third party. In the latter case, a substantial element of trust is involved, not only that the third party will do only what you’ve authorized but that this party won’t give away either deliberately or accidently authenticators that enable their remote access.

We can also imagine a range of authorized actions so that we could give authority for some

Vinton G. Cerf

cont. on p. 95
actions but not others. For example, you might authorize monitoring of the status of a device or appliance but not control over its state. Of course, the more options that are available, the more complex the configuration process could be. For anyone who has had to manage a long list of account identifiers and authenticators, it isn’t hard to see how all of this could quickly get out of control. How do you revoke access to an appliance? How do you even remember to do it? Do you need to be reminded periodically who has access and asked whether you intend to maintain this privilege? How should you be notified if there is a breach of some kind? How would this even be detected? Will you have to peruse logs of access and action yourself? Will software look for potential abuse? What will be done about false positives? Do we really want a text message from the refrigerator announcing that it thinks it’s been violated? Will we have to pass laws about abuse of other people’s appliances?

My purpose isn’t to paint a particularly dark future, although it isn’t hard to see that possibility. Rather, I hope to draw attention to the need for some serious thought about managing an Internet of Things. It will call for some extraordinarily thoughtful user experience design, to say nothing of very robust access controls and strong authentication, resilience, and recovery procedures. It’s bad enough that we have to reset a collection of clocks twice a year manually where daylight savings time is observed. Maybe we could fix that annoyance while we’re working on the other tricky aspects of “thing management”?

Vinton G. Cerf is vice president and chief Internet evangelist at Google. Contact him at vint@google.com.