What Was Samsung Thinking?

Susan Landau
Associate Editor in Chief

In February 2015, the press discovered that if Samsung's Smart TV voice recognition system is activated, the television sends voice commands to Samsung and then to a third-party provider for processing. Any other conversations that are overheard are also sent. The company's user manual explains:[1]

> If you enable Voice Recognition, you can interact with your Smart TV using your voice. To provide you the Voice Recognition feature, some voice commands may be transmitted (along with information about your device, including device identifiers) to a third-party service that converts speech to text or to the extent necessary to provide the Voice Recognition features to you.

This is no different from how Siri works. Google Glass is slightly different; it transmits your voice commands to Google but apparently no further. Yet, years after those products launched, Samsung's Smart TV raised quite the brouhaha. The story was all over CNN, ABC, BBC, and the *Washington Post,* and there was a Congressional hearing. The Electronic Privacy Information Center filed a complaint with the Federal Trade Commission, seeking a prohibition on the product's recording and transmitting voice communications and a determination of whether Samsung violated the Electronic Communications Privacy Act, which prohibits "interception and disclosure of wire, oral, or electronic communications."[2]

One problem with the product is that Samsung misled its customers. It claimed the voice communications were encrypted, but researchers at Pen Test Partners found otherwise.[3] Transmissions from the TV's early models were sent in the clear. Furthermore, Samsung doesn't appear to have addressed data collection security: how data would be transmitted and stored, who would have access to the data, how long it would be kept, and what third-party security practices would be.

These security concerns are complicated, but they are ones that engineers have been trained to tackle. The real issue is how we employ devices. This is different from the concern about the voice channel being hacked.

Privacy Expectations and Social Context

People use smartphones to make a call, check their email, or look for directions. Although smartphones transmit users' location to the network, the assumption is that if a phone isn't actively being used, only location information is transmitted. (Yes, we've all seen the television show in which a cell phone is surreptitiously used to tape a conversation. That's considered a misuse of the phone and is a violation of social protocol.) The same is true of Google Glass. In fact, when users ask Glass to perform an action such as taking a photo, they must say, "Okay, Glass," and a small red light comes on to indicate transmission. When users give Samsung's Smart TV a voice command, there's no transmission unless users click an activation button on the remote control or TV screen and speak into the microphone on the remote control.[4] The voice is transmitted only while the control system is activated. In this way, Samsung's voice recognition technology works much the same as Siri and Glass.

Asking Siri a question or saying "Okay, Glass" might be unnoticeable in a crowded room—many activities are. People assume they will be observed in busy, noisy spaces. But privacy is taken for granted at home. TVs are literally pieces of furniture that fade into the background (many times they are, in fact, on in the background). This mismatch is what caused the vehement reaction to Samsung's product.

When we're busy chopping vegetables for dinner, helping a child with homework, negotiating tomorrow's chores, or getting ready for bed, we don't want—or anticipate—these discussions to be picked up along with "Recommend a good sci-fi movie" and sent to Samsung and its processing partner, Nuance Communications. The conversations might not be particularly confidential, but sharing

1540-7993/15/$31.00 © 2015 IEEE Copublished by the IEEE Computer and Reliability Societies May/June 2015

them makes us uncomfortable. This is exacerbated by the fact that, at home, we're often not paying enough attention to notice when the Smart TV voice recognition system is in use. Televisions are in sensitive locations: living rooms, bedrooms, hotel rooms. They're inevitably plugged in and often left on—sometimes just to tell time. That's the concern.

There's a design disconnect going on. Engineers see Samsung's voice recognition as an electronic system and consider efficiency and bandwidth. Anthropologists see Samsung's Smart TV and recognize that Samsung's voice recognition system is an artifact that transmits conversations from one social space to another. That shift of social space is surprising. Put this way, the problem is clear.

Designing Privacy into IoT Systems

It's obvious that Samsung didn't carefully think through the use case of Smart TVs. But there's a deeper issue. The Samsung Smart TV example points out how the Internet of Things (IoT) must transform the way we design Internet-mediated systems.

The knotty issues concern the devices' social context. How do people perceive the space in which a smart device is being used? What are users' expectations for privacy in a room with a television? What is the expectation of the other people in range of a microphone—for instance, those oblivious to a television being on?

These are the kinds of questions social scientists ask, and they're important in smart TV system design. They don't arise in the design of every IoT system—for example, sensors collecting soil humidity data don't raise large concerns about privacy. But they're important for IoT systems that potentially monitor people, including their use and interaction with the system. This includes smart thermostats, smart lightbulbs, smart refrigerators, and smart meters.

Samsung doesn't seem to have raised questions about how televisions function inside homes. Asking these types of questions is a crucial first step in building more privacy-protective IoT systems. Learning that many, if not most, people don't want to transmit their background conversations to Samsung and third parties, the company must make tradeoffs when redesigning its Smart TV product. Can it build a system that computes the information locally? If such a solution is technically infeasible at present, does Samsung need to create a more in-your-face notice every time a conversation is being transmitted from the room?

When designing a communications device, it's natural to ask about communication expectations. What are the expectations about delivery, privacy, security, and accuracy? But IoT is different—we're talking about taking everyday devices and having them communicate on the network.

Consider another IoT concern—this one involving phones. Smartphone sensors can collect ambient noise that can be used to figure out where users are. This isn't GPS data—whether a user is at 17 South Maple Street—but information that locates users in a very different way: in a bar, at a meeting, in a car.[5] Does this information have value? Sometimes. When someone is in a crowded bar, perhaps the phone volume should increase automatically. When someone is in a meeting, perhaps the phone should automatically switch to vibrate mode. When a person is in a car, perhaps texting capability should be shut off—though not when the user is a passenger.

One could imagine good reasons for information determining locale to be transmitted, but the privacy issues are quite serious. What mental model do people have about information their phones transmit about them? And what about the people nearby—for instance, those in the same meeting? How would they feel about the fact that someone else's phone is transmitting information about them, even though it's ostensibly not being used?

If we hope to provide an IoT world that's useful, rather than one in which people must shut off their devices to achieve a desired level of privacy, we must understand users' expectations of their devices. Samsung's Smart TV situation throws that into clear relief. This situation could be a wake-up call, causing companies to realize that they must delve into how devices actually function in peoples' lives, and then build accordingly. If so, Samsung's Smart TV will have taught a very useful lesson. ■

References

1. "Samsung Privacy Policy—SmartTV Supplement," Samsung, 10 Feb. 2015; www.samsung.com/us/common/privacy.html#smart.
2. 18 US Code § 2511—Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited, US Code Title 18, Part I, Chapter 119, 3 Jan. 2012.
3. D. Lodge, "Is Your Samsung TV Listening to You?" Pen Test Partners blog, 16 Feb. 2015; www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you.
4. "Samsung Smart TVs Do Not Monitor Living Room Conversations," Samsung Tomorrow, 10 Feb. 2015; http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations.
5. V. Narayanan, S. Nanda, and F. Shih, "Learning Situations via Pattern Matching," US 20120265717 A1, US Patent Office, 18 Oct. 2012.