# Your Device Can Spy On Your Every Move

Do you really know for sure your GPS is off simply because your phone's screen says it is?
**H V Jagadish, The Conversation | 27 April 2016 00:05**


We now have dozens of smart devices in our houses and even on our bodies. They improve our lives in so many ways – from lowering energy consumption in our homes to egging us on to be active.

But these smart devices respond to whatever commands they are given: we've had security experts demonstrate how cars can be hijacked remotely and medical devices in your body can be hacked and turned into lethal weapons. These risks are now well-recognized by technology developers, and there is a great deal of excellent work going on toward how to avoid them.

But there are other dangers we should be more concerned about that are getting less attention. Your gadgets could be providing a window that any hacker could see right through to spy on you.

## Your stuff is surveilling you

Your laptop has a video camera built into it. When it's recording, a little green light blinks on so you're aware you're being recorded. But it can be instructed to videotape your activities without the green camera light being on. And this is not just an in-laboratory

warning of a hypothetical danger; it has actually been done, by over-eager school officials and by peeping Toms.

At least you can turn off your laptop: when it is shut, the camera can see only "the other side" of the laptop. But this quick fix doesn't apply to sound recording devices, like microphones. For example, your phone could listen to conversations in the room even when it appears to be off. So could your TV, or other smart appliances in your home. Some gadgets – such as Amazon's Echo – are explicitly designed to be voice activated and constantly at the ready to act on your spoken commands.

It's not just audio and video recording we need to be concerned about. Your smart home monitor knows how many people are in your house and in which rooms at what times. Your smart water meter knows every time a toilet is flushed in your home. Your alarm clock knows what time you woke up each day last month. Your refrigerator knows every time you filled a glass of cold water. Your cellphone has a GPS built into it that can track your location, and hence record your movements. Yes, you can turn off location tracking, but does that mean the phone isn't keeping track of your location? And do you really know for sure your GPS is off simply because your phone's screen says it is? At the very least, your service provider knows where you are based on the cellphone towers your phone is communicating with.

We all love our smart gadgets. But beyond the convenience factor, the fact that our devices are networked means they can communicate in ways we don't want them to, in addition to all the ways that we do.


Is this thing on? Amazon.com, Inc

# Next generation wiretapping

A bad actor could figure out how to take control of any of these technologies to learn private information about you. But maybe even more worryingly, could your technology provider become, voluntarily or under compulsion, a party to a scheme through which you unwittingly reveal your secrets?

The recent battle between Apple and the FBI revolved around the feds' request that Apple develop a custom insecure version of iOS, the operating system of the iPhone, to facilitate their hacking into a terrorist's cell phone. Is breaking into a locked phone just the next step beyond a traditional wiretap in which the government asks an Apple or a Samsung to use its technology to bug the conversations of a suspected terrorist?

But modern phones can be used to do a lot more than listen in on conversations. Could companies be asked to keep location tracking on while indicating to the suspect that it is really off? It would seem to me hard to draw a line between these cases. No wonder some Apple engineers came out as "objectors of conscience" in the Apple-FBI matter. This case was dropped before Apple could be compelled to do anything, so there's no legal precedent to guide us on how these next-step examples would play out in court.

It is, of course, valuable for law enforcement to monitor criminal suspects, to investigate ongoing criminal behavior and to collect evidence to prosecute. This is the motive behind wiretap laws that allow law enforcement to listen to your phone conversations with no notice to you.

Wiretaps actually got their start in the 1800s as tools of corporate espionage. In 1928, the U.S. Supreme Court ruled in Olmstead v. U.S. that it was constitutional for law enforcement to use wiretaps, and that warrants weren't required. This decision was superseded only in 1967, by Katz v. U.S., which established a citizen's right to privacy, and required law enforcement to obtain warrants before bugging a phone conversation. This was long after Congress had passed an act carefully restricting wiretaps, in 1934.

In the early days of wiretapping, there was a physical "tap" – a side connection – that could be applied to a real wire carrying the conversation. Newer technologies eventually permitted the telephone company to encode and multiplex many telephone calls on the same physical wire.

Technology has moved on, but the law isn't clear yet. Gawler History, CC BY-SA

In the United States, the Communications Assistance for Law Enforcement Act (CALEA) was passed by Congress in 1994, due to worries about law enforcement's ability to keep up with new communications technologies. It requires communication companies to provide a way for law enforcement to place a wiretap even on newer communication technologies.

The law explicitly exempted information services, such as email. This legal differentiation between communications technologies and information services means companies are obliged to help the government listen in on your phone calls (with a warrant) but are not obliged to help it read your email messages (at least on account of this specific law).

In 2004, the Federal Communications Commission ruled that services such as Voice Over IP (think Skype) were communications services covered by CALEA, and not exempt information services.

Some have since wanted to further broaden this law, and doubtless the Apple FBI dispute brings this issue to the forefront again. Law enforcement will presumably push for greater surveillance powers, and civil liberty advocates will resist.

## Nothing to hide?

Perhaps you don't care about the privacy of criminals. But note that surveillance is not just of *known* bad actors, but also of *suspected* bad actors.

History teaches us that lists of suspects can sometimes be drawn way too broadly. You may remember the McCarthy era and J. Edgar Hoover's reign at the FBI, which infamously included bugging Martin Luther King Jr.'s bedroom. Even today, there are attempts by the British Government Communications Headquarters to monitor everyone who visited the Wikileaks website, even just to browse. Some laws don't make sense or aren't fair, so even some "criminals" may still deserve privacy.

And it's not just law enforcement overreach we have to worry about. Technologies like Finspy are commercially available today to install malware on your computer or phone and "recruit" it to spy on you. Such technologies could be used by anyone, including the "bad actors," without the cooperation of your device manufacturer or service provider.

Wiretap laws, such as CALEA, apply to explicit communication actions taken by someone, such as actually making a phone call. Wiretaps do not track your movements in the house, they do not listen to your conversations when you are not on the phone, they do not videotape you in your bathroom – but these are all actions our various devices are now capable of performing. With the proliferation of devices in our lives, it is certainly possible to use them for surveillance purposes. There's no question that by doing so, authorities will catch many bad actors. But there will also be a huge price to pay in terms of privacy and possibly wrongful arrests.

Finally, this may feel futuristic, but I assure you it is not. The FBI was already using a cellphone microphone to eavesdrop on organized crime as long as a decade ago. Commercial interests are not too far behind in doing much the same, with the purpose of targeting a better sales pitch.

Our omnipresent networked devices raise big questions that we should openly debate. How we balance these costs and benefits will determine the type of society we live in.

H V Jagadish, Bernard A Galler Collegiate Professor of Electrical Engineering and Computer Science, *University of Michigan*

This article was originally published on The Conversation. Read the original article.