



Jan. 21, 2014, 7:09 a.m. EST

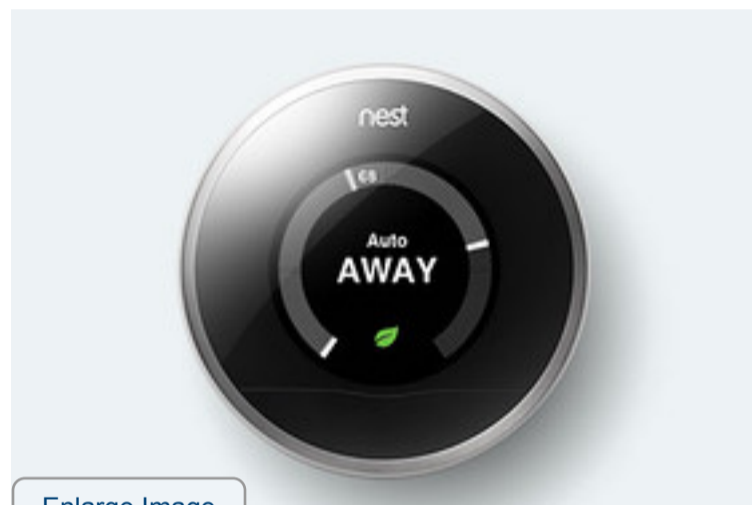
## Your home will soon be one giant iPhone

Google (and others) know when you're asleep — and when you're awake

By **Quentin Fottrell**

**Google's (NASDAQ:GOOG) purchase of home automation company Nest Labs gives the world's biggest search engine a foothold in people's homes. But experts say Internet companies are already tracking the habits of Americans at home — and it's only just begun.**

On Monday, Google said it paid \$3.2 billion for Nest, a maker of smartphone-controlled thermostats and smoke alarms. Founded in 2010 by two former Apple (NASDAQ:AAPL) employees, Tony Fadell and Matt Rogers, the company's \$249 "next generation" thermostat learns your schedule and even programs itself when you're not home. The thermostat industry has about \$3 billion in annual revenue, according to industry research firm IBISWorld, up 2% annually since 2008. But the market for smartphone-operated household appliances is estimated to surge from \$612 million in 2012 to \$35 billion in 2020, according to Navigant Research. "Smartphones are increasingly the remote controls for our lives," says Jeff Kagan, a technology analyst. "They will control everything in your house and car."



Enlarge Image

Nest Labs

"You can expect to see more companies attempting to do this in coming years, tracking nearly every movement in your home," says Neil Strother, senior research analyst at Navigant Research. There is already a small army of apps doing just that. SmartThings, a free app for iOS and Android, monitors light switches, unlocked doors and car keys. Home automation company [Vivint](#), bought for \$2 billion by Blackstone Capital Partners in 2012, says it services 800,000 customers in North America. Its free iOS app can act as a motion detector, remote-controlled security system and electronic door lock. [AT&T's Digital Life](#) offers plans from \$4.99 per month that track water leaks, energy usage, unlocked doors and home security cameras. Tech company Belkin even launched a [smartphone-controlled slow cooker](#).

How does this affect your privacy? What companies learn when you check in at a restaurant on [Facebook](#) or plug your location into Google Maps pales in comparison to the wealth of data that they'll glean from (and possibly use against) consumers in the not-so distant future, says Adi Kamdar, an activist at the non-profit Electronic Frontier Foundation, a consumer advocacy group focusing on online privacy. "Connected cars may report unsafe driving, raising or canceling your insurance," he says. Similarly, a home insurance company might be interested in a smoke detector that goes off several times a day. "During a divorce, your spouse subpoenas a thermostat company for records to prove that you set low temperatures in the house, keeping your kids too cold. Is that something you want to even deal with?" he asks.



### How does Google benefit from Nest deal?

Dan Gallagher joins MoneyBeat with a look at how Google's deal for Nest Labs will pay off. Photo: Nest Labs.

Most companies aggregate data, but say they don't release personalized information. In a blog on the [company's website](#), Nest co-founder Matt Rogers writes, "Our privacy policy clearly limits the use of customer information to providing and improving Nest's products and services." Google's privacy policy constantly evolves. It's nearly increased fourfold in size from 650 words a dozen years ago to [2,260 words today](#): "We may share aggregated, non-personally identifiable information publicly and with our partners — like publishers, advertisers or connected sites," it states. Similarly, SmartThings' privacy policy states, "We may also provide aggregate information to our partners." And [Vivint's privacy policy](#) states that it doesn't sell or trade personally identifiable information — except to "trusted third parties" and to comply with the law.

Nor does potential use of consumer data take into account data hacking. "What happens if someone gets into your phone?" says Rick Singer, CEO of GreatApps.com. Or into your smart meter? In 2011, German researchers Dario Carluccio and Stephan Brinkhau gave a [presentation](#) about accessing the unencrypted data passing from smart meters to a utility company's server. After two days of analyzing data, they were able to tell whether the householder was at home, away or asleep, how many personal computers and TVs were in the home, and even what he or she was watching on television. TVs and computer cameras are also vulnerable to hacking, says Adam Levin, co-founder of online security company Identity Theft 911. In 2012, for instance, Samsung fixed a bug in its Smart TV after Malta-based security company [ReVuln](#) turned on a TV's built-in security camera. ■