20 Aug 2020 | 15:00 GMT

# For the IoT, User Anonymity Shouldn't Be an Afterthought. It Should Be Baked In From the Start

The best way to avoid mass surveillance is to build systems that don't collect personal data in the first place

By **Stacey Higginbotham**

Illustration: Greg Mably

**The Internet of Things** has the potential to usher in many possibilities—including a surveillance state. In the July issue, I wrote about how user consent is an important prerequisite for companies building connected devices. But there are other ways companies are trying to ensure that connected devices don't invade people's privacy.

Some IoT businesses are designing their products from the start to discard any personally identifiable information. Andrew Farah, the CEO of Density, which developed a people-counting sensor for commercial buildings, calls this "anonymity by design." He says that rather than anonymizing a person's data after the fact, the goal is to design products that make it impossible for the device maker to identify people in the first place.

"When you rely on anonymizing your data, then you're only as good as your data governance," Farah says. With anonymity by design, you can't give up personally identifiable information, because you don't have it. Density, located in Macon, Ga., settled on a design that uses four depth-perceiving sensors to count people by using height differentials.

Density could have chosen to use a camera to easily track the number of people in a building, but Farah balked at the idea of creating a surveillance network. Taj Manku, the CEO of Cognitive Systems, was similarly concerned about the possibilities of his company's technology. Cognitive, in Waterloo, Ont., Canada, developed software that interprets Wi-Fi signal disruptions in a room to understand people's movements.

With the right algorithm, the company's software could tell when someone is sleeping or going to the bathroom or getting a midnight snack. I think it's natural to worry about what happens if a company could pull granular data about people's behavior patterns.

Manku is worried about information gathered after the fact, like if police issued a subpoena for Wi-Fi disruption data that could reveal a person's actions in their home. Cognitive does data processing on the device and then dumps that data. Nothing identifiable is sent to the cloud. Likewise, customers who buy Cognitive's software can't access the data on their devices, just the insight. In other words, the software would register a fall, without including a person's earlier actions.

"You have to start thinking about it from day one when you're architecting the product, because it's very hard to think about it after," Manku says. It's difficult to shut things down retroactively to protect privacy. It's best if sensitive information stays local and gets purged.

Companies that promote anonymity will lose helpful troves of data. These could be used to train future machine-learning models in order to optimize their devices' performance. Cognitive gets around this limitation by having a set of employees and friends volunteer their data for training. Other companies decide they don't want to get into the analytics market or take a more arduous route to acquire training data for improving their devices.

If nothing else, companies should embrace anonymity by design in light of the growing amount of comprehensive privacy legislation around the world, like the General Data Protection Regulation in Europe and the California Consumer Privacy Act. Not only will it save them from lapses in their data-governance policies, it will guarantee that when governments come knocking for surveillance data, these businesses can turn them away easily. After all, you can't give away something you never had.

*This article appears in the September 2020 print issue as "Anonymous by Design."*

**Suggested Wiley-IEEE Reading**