Internet of Things will transform life, but experts fear for privacy and personal data

November 5 2014, by Steve Johnson, San Jose Mercury News

It will help you avoid traffic jams as you travel from work to that hot new spot you've been dying to try out, tell you on the way about the bar's half-price coupons and let you check your home video monitors while knocking back a few to see if your cat is clawing the couch again.

But it also might alert your insurer if your car is weaving when you head home and report your frequent drinking to your boss.

"It" is the Internet of Things, which promises to transform daily life, making it easier to work, travel, shop and stay healthy. Thanks to billions of connected devices - from smart toothbrushes and thermostats to commercial drones and robotic companions for the elderly - it also will end up gathering vast amounts of data that could provide insights about our sexual habits, religious beliefs, political leanings and other highly personal aspects of our lives. That creates a potentially enormous threat to our privacy - even within the sanctuary of our homes.

"These are incredibly convenient devices," said University of Colorado law professor Scott Peppet, who has extensively researched the Internet of Things. "They are magical."

Nonetheless, he added, "I don't think we're being overly reactive to say, 'Wait a minute, what are the constraints on using that information? I just want to know what you are going to do with my data.' "

Just what happens to the data spewed out by all these interlinked

machines is a deep concern shared by many security researchers, legal authorities, government officials and consumer advocates. They fear the information could be used to skew our credit ratings, jack up our insurance rates, help hackers steal our money, or enable spy agencies to compile detailed dossiers on each of us. Moreover, they say, this vast sea of data could be misused to put a high-tech twist on the age-old curse of discrimination, with unscrupulous landlords or employers excluding people based on the data they've secretly acquired.

The technology is quickly becoming reality, with scores of helpful smart devices already on the market, including some from Bay Area companies.

Sensors from San Francisco-based Lively alert relatives when an older family member fails to take medicine, eat or return home from a walk. Nest thermostats from Google in Mountain View, Calif., learn and automatically adjust to how warm or cool their owners want their houses. Mobile robots from Suitable Technologies of Palo Alto, Calif., feature screens that let people video conference from various locations. And dog owners can remotely check on what their pooches are doing with a smart collar by Whistle of San Francisco.

Among other advantages, the devices are widely expected to improve public health by keeping patients in closer touch with doctors, reduce highway deaths by automatically braking vehicles to avoid crashes, boost food supplies by helping farmers tend their crops, and quickly notify authorities about environmental mishaps. When the nonprofit Pew Research Center queried more than 1,600 experts on the subject, 83 percent predicted the Internet of Things will "have widespread and beneficial effects on the everyday lives of the public by 2025."

Yet, with devices from cars to refrigerators to coffee pots recording everything we do and transmitting the information to others, many

people may find the technology unnerving.

"The idea that when I'm in my house or on my property or in my car, I'm somehow in a surveillance-free zone - no, it's not true," said Electronic Frontier Foundation attorney Lee Tien. "We're seeing just a tremendous explosion of surveillance."

Although people already reveal much about themselves through their Internet searches and social media posts, that's nothing compared with the trove of personal data likely to be disclosed by the Internet of Things.

Even when designed for limited functions, experts say, many of these Web-linked gadgets will record whatever they see and hear in homes, which could provide detailed dossiers on the people living there, especially when combined with what's amassed by other interconnected machines. The personal data revealed could include everything from your friends, hobbies and daily routines to your political views, religious affiliation and even your sexual activities.

Your politics might be disclosed if you routinely watch like-minded programs on your Web-connected TV and use your personal robot's videoconferencing capabilities for online meetings with a group that shares your views. And if you've declared your political allegiance in private comments, your voice-activated gadgets might have picked those up and stored them as text on the Internet.

Your religious orientation, on the other hand, might be divulged by your Internet-linked refrigerator. Because those appliances are expected to become so smart they'll automatically order more eggs, beer or other items for you when supplies run low, yours might signal that you're Jewish, for example, if it frequently gets you kosher food.

Still other gadgets might put your love life on display if, for instance, you pick up someone you meet at that new bar after work.

That's conceivable if your home security camera tapes the two of you undressing and its face-recognition software determines your date is a prominent local official, while your wearable fitness device calculates from the calories you proceed to burn that you must be having sex. Disclosing those details could prove embarrassing, especially if you're both married. It could be even more so if your wireless health monitor a week later fires off an alert to your doctor that you've just contracted a sexually transmitted disease.

So how could others see that personal information?

Much of it is expected to flow directly from the gadgets to the businesses that made them. Legal experts say federal and state laws poorly regulate how the information can be used, and the companies already selling smart gadgets often are vague about what they do with the data or whether they sell it to others. Consequently, it's possible someone's personal details could bounce around the Internet and be accessed by countless people.

Such firms often say they "de-identify" the data so it can't be attributed to individuals. Yet researchers have found it's frequently possible to "re-identify" data by combining it with other available facts. As a result, a White House report in May concluded that data re-identification "creates substantial uncertainty" about peoples' ability to control their personal information.

That raises another red flag for the administration and experts in the field. The White House study warns that the growing deluge of data could result in "discriminatory outcomes for disadvantaged groups."

It's illegal to discriminate against anyone based on their race, color, religion, national origin or sex. But given the uncertainty about who might see the information disgorged by these smart gadgets, it's widely feared the data might be used to treat people unfairly without their knowledge. For example, experts say, a person might get turned down for an apartment if their devices reveal their sexual or religious orientation to a disapproving landlord.

It's also conceivable employers might refuse to hire someone after learning from the person's medical or fitness gadgets that they've got a health problem, said Rebecca Herold, a privacy consultant and adjunct professor at Norwich University in Vermont. Moreover, while banks and other creditors generally are prohibited from inquiring about a loan applicant's sex and race, she said, they might "turn down a loan to such an individual" after surreptitiously learning those details from the applicant's devices.

All this worries Federal Trade Commission Chairwoman Edith Ramirez.

"Will the data transmitted be shared with your insurer, who may raise your rate or cancel your policy?" she wondered aloud during a conference on the Internet of Things. "Will your TV viewing habits be shared with prospective employers or schools or with data brokers, who will put that nugget together with information collected by your parking-lot security gate, your heart monitor and your smartphone, and paint a picture of you that you won't see, but that others will?"

Among those hoping to gain access to the information are advertisers. They plan to parse it for details about consumers so they then can pitch them products tailored to their individual preferences via their brainy gadgets, which could result in people's homes being deluged with ads. In a regulatory filing, Google forecast that "a few years from now, we and other companies could be serving ads and other content on refrigerators,

car dashboards, thermostats, glasses and watches, to name just a few possibilities."

Insurance companies also are likely to seek the data.

Thousands of motorists already voluntarily let such firms use smart-car devices to check their driving, including whether they speed or take violent turns. And with so many other gadgets revealing every facet of how people live, experts say, much of that information is bound to get factored into health and home insurance, perhaps on a mandatory basis.

If that leads to healthier lifestyles and safer residences, it will likely gain acceptance, said insurance consultant Fred Cripe. Even so, he added, "As with anything, there's going to be some resistance."

Some experts fear the data gathered and shared by all these computerized gadgets also could make it easier for the government to spy on U.S. citizens. Despite the Fourth Amendment's prohibition on unreasonable searches and laws that limit domestic snooping, civil rights groups claim that police and other government agencies in recent years have increased their monitoring of Americans in the name of national security. And in a speech two years ago, former CIA Director David Petraeus predicted that the Internet of Things could have a significant impact "on clandestine tradecraft" by enabling "near-continuous, persistent monitoring of virtually anywhere we choose."

Petraeus didn't say whether that might happen in the U.S. But because of ambiguities in the law about who can see data gathered by smart devices, experts say, conflicts over access to the information could spark legal battles in this country.

"A lot of this is going to have to be hashed out in the courts," said James Quiggle of the Coalition Against Insurance Fraud, whose members

include police and prosecutors. "This is huge. You're talking about Big Brother issues."

Another worry is that the technology could spark a surge in crime. Many existing medical devices, cars and other connected gear have been found vulnerable to hackers, who already have caused numerous high-profile data breaches. And as those devices multiply, experts fear, so do the opportunities for cybercrooks to snatch financial or other information belonging to vast numbers of people.

"The risk is real," Mountain View security firm Symantec recently reported, warning that "Internet of Things devices will become access points for targeted attackers."

Nonetheless, the technology is exploding, with research firm IDC predicting that smart, Internet-linked objects will number more than 200 billion and generate in excess of $7 trillion in annual sales by 2020.

Among the early adopters is Tom Coates, a 42-year-old former Yahoo technologist and co-founder of Product Club, which develops inventions. He has filled his San Francisco home with smart gadgets, including lights he activates by phone, a video camera that lets him remotely watch over his house, a bathroom scale that tweets his weight, and sensors that warn of intruders and track the health of his yucca plant.

But Coates believes it's prudent to be mindful of both the good and bad that can result from the technology.

"We need to look at its benefits" while also making sure to "look at the risks and minimize them," he said. "We have to be part of the process of making the Internet of Things something that helps people and saves lives without damaging human rights."

—-

TATTLETALE GADGETS

These are examples of Internet-of-Things devices that experts fear might reveal personal data about their users:

-Web-connected TV: By recording what programs you watch, it could reveal everything from your sexual preferences to your political leanings.

-Personal robot: Its voice-activated feature might record and disseminate to the Internet comments you make about your friends, neighbors, boss and others.

-Smart refrigerator: Could show how much beer and wine you drink, as well as your religious affiliation, if, for example, you regularly buy kosher food.

-Home security camera: May reveal who your friends are, what you look like when undressed and even your sexual practices.

-Wearable fitness devices: Could report whether you are out of shape.

-Portable heart or other health monitors: Possibly disclose all your medial ailments

-Smart washing machine: By reading radio-frequency identification tags sewn into your clothes, it might disclose your waist-size, style of clothes you wear, and if someone from the opposite sex lives with you.

-Smart vacuum: Could show how often you clean your carpets and how grimy your house is.

-Utility smart meters: By recording the electricity use of households, they could reveal when the residents get up and go to bed, what types of electric devices they have and which ones they're using at any given moment.

©2014 San Jose Mercury News (San Jose, Calif.)
Distributed by MCT Information Services

Citation: Internet of Things will transform life, but experts fear for privacy and personal data (2014, November 5) retrieved 16 August 2024 from https://phys.org/news/2014-11-internet-life-experts-privacy-personal.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.