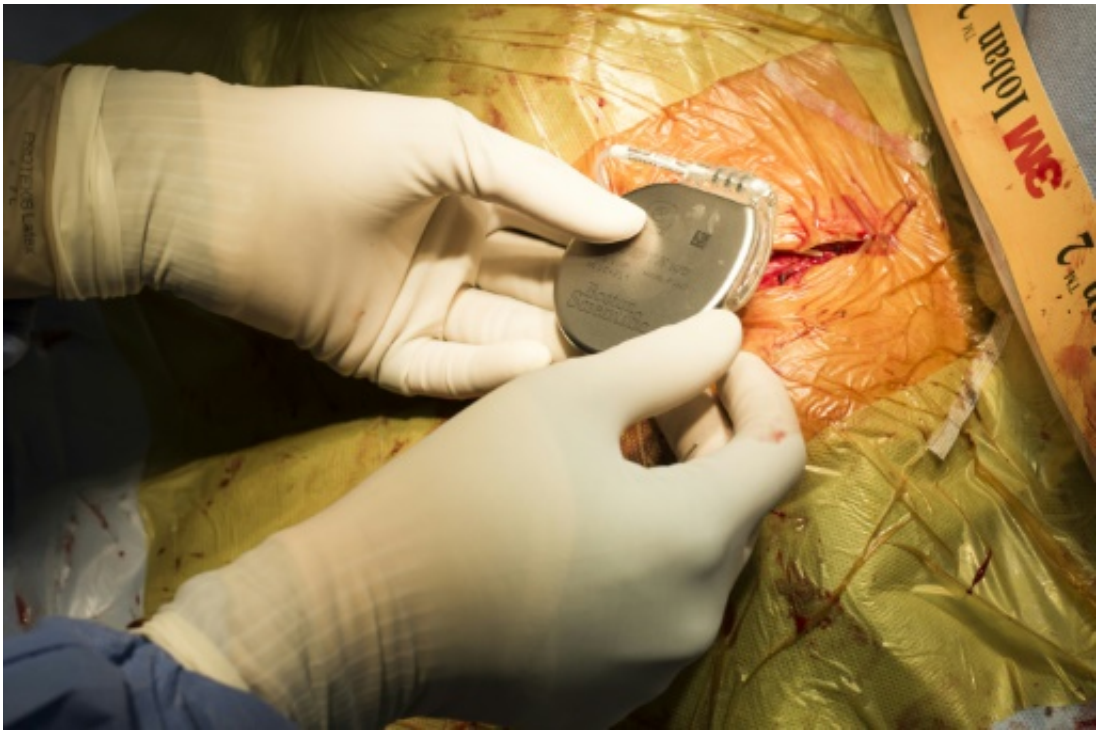
Secrets from smart devices find path to US legal system

March 19 2017, by Rob Lever



A surgeon implants a pacemaker to a patient

An Ohio man claimed he was forced into a hasty window escape when his house caught fire last year. His pacemaker data obtained by police showed otherwise, and he was charged with arson and insurance fraud.

In Pennsylvania, authorities dismissed rape charges after data from a woman's Fitbit contradicted her version of her whereabouts during the

2015 alleged assault.

Vast amounts of data collected from our connected devices—fitness bands, smart refrigerators, thermostats and automobiles, among others—are increasingly being used in US legal proceedings to prove or disprove claims by people involved.

In a recent case that made headlines, authorities in Arkansas sought, and eventually obtained, data from a murder suspect's Amazon Echo speaker to obtain evidence.

The US Federal Trade Commission in February fined television maker Vizio for secretly gathering data on viewers collected from its smart TVs and selling the information to marketers.

The maker of the smartphone-connected sex toy We-Vibe meanwhile agreed in March to a court settlement of a class-action suit from buyers who claimed "highly intimate and sensitive data" was uploaded to the cloud without permission—and shown last year to be vulnerable to hackers.

'Privacy is dead'

Trying to come to grips with data collected, stored and analyzed by all these devices can be daunting.

"When one looks at the expectation of privacy today it is radically different than it was a generation ago," said Erik Laykin, a digital forensics specialist with the consultancy Duff & Phelps and author of a 2013 book on computer forensics. "Privacy is dead."

Laykin has consulted or testified in cases of insurance fraud, divorce and other legal proceedings where digital evidence can be relevant.

He said the "always on" nature of "internet of Things" devices means huge amounts of personal information is circulating among companies, in the internet cloud and elsewhere, with few standards on how the data is protected or used.

"The net result of these technologies is that we are forgoing our personal privacy and our personal autonomy and even sovereignty as humans and relinquishing that to a combination of state, harvesters of big data, omnipresent institutions and systems."

A report last year from Harvard's Berkman Klein Center for internet studies pointed out the range of new connected devices that can yield evidence for law enforcement, "ranging from televisions and toasters to bed sheets, light bulbs, cameras, toothbrushes, door locks, cars, watches and other wearables," which "are being packed with sensors and wireless connectivity."

"The audio and video sensors on IoT devices will open up numerous avenues for government actors to demand access to real-time and recorded communications," the report said.

John Sammons, a Marshall University professor of digital forensics and a former police officer, said this new abundance of evidence can be good for law enforcement if investigators can find relevant data.

"You have to be aware it's even there," he said.

"Most police officers would not even think to look at a Fitbit or a thermostat."

Another problem is the sheer volume of data and computing resources needed to obtain specific data, often requiring weeks of computing time.

Sammons presented research on use of connected cars this year at the American Academy of Forensic Sciences, saying newer vehicles with improved connectivity offer "a significant new source of potential evidence" for both criminal and civil litigation.

Privacy in the cloud?

Privacy activists meanwhile worry that these devices can unleash new kinds of surveillance without the knowledge of users, and that the legal system must define limits for constitutional protections against unreasonable searches.

Jay Stanley of the American Civil Liberties Union's Speech, Privacy, and Technology Project, said gathering data from connected speakers such as the Amazon Echo should face the same standard as wiretaps, which need a warrant from a judge based on probable cause of a crime, rather than a more streamlined law enforcement subpoena.

"In your house you should have absolute privacy," Stanley said.

One gray area in the law is that conversations recorded on home speakers may be sent to the cloud; in that case the holding of the data by a "third party" may wipe away constitutional privacy protection.

"We think there needs to be jurisprudential and legislative means of addressing these issues," Stanley said. "The privacy invasions are so significant."

Jules Polonetsky, chief executive of the non-profit Future of Privacy Forum, said that while legal issues are still being debated, "you should always know if you have a device that is sending data elsewhere."

Polonetsky said it's important to set a legal and constitutional privacy

framework to reassure consumers.

"It's critical we get the balance between data utility and law enforcement access right," he said, "or people won't trust these devices."