LOCAL NEWS

Help Squad: Health insurers and other corporations analyze our plentiful personal data, then devise ways to profit from findings

Karen Bleier/ Getty Images

Some health insurers are purchasing personal data from brokers who track things like visits to social networking sites, web browsing histories and consumer purchases.

By CATHY CUNNINGHAM

PUBLISHED: August 29, 2018 at 11:20 a.m. | UPDATED: December 12, 2018 at 10:24 p.m.

I recently read a ProPublica article that both concerned me and inspired me to learn more. It was titled "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates."

How are insurers doing this? According to the post, health insurance companies are now purchasing information from data brokers — companies that collect public and private information on all of us from social networking sites, web browsing histories, consumer purchases, census data, court and driving records and health-based service providers, to name just a few.

Is it legal? As explained by William McGeveran, University of Minnesota professor of law, and Craig Konnoth, University of Colorado associate professor of law, it is — largely because federal law hasn't kept pace with the modern, technological world in which we live.

Said McGeveran, "The law is really structured for a non-social media, non-digital information world. It is dated in lot of important ways."

Unlike in Europe, where the General Data Protection Regulation (GDPR) (www.eugdpr.org) became law in May, in the United States, the baseline assumption is that companies can collect, use and sell as much personal information as they wish, unless the law specifically prohibits it.

There are two key exceptions to this Wild West approach to buying and selling personal data, however, said Konnoth:

— The Genetic Information Non-discrimination Act (GINA), which prohibits health insurers from denying coverage or charging higher premiums to individuals identified with a genetic predisposition to future disease.

— The Affordable Care Act (ACA), which states that health insurance companies cannot refuse coverage or charge higher premiums because an individual has a pre-existing condition.

He additionally told me that "covered entities," which include medical providers, insurers and other companies that play in the medical space, cannot share individuals' identifying data with any other organizations. However, non-covered entities such as Facebook and IMS Health — one of the largest data brokers providing information to the health care industry — are not limited by these HIPAA (Health Insurance Portability and Accountability Act) restrictions, and as such can collect and sell personal data as they wish.

"In Europe, GDPR requires a legitimate justification for collecting and processing personal information," explained McGeveran. "There is an explicit list of reasons a company can collect (personal information), and it must provide one of the reasons on that list in order to use it."

He continued, "In the United States, everything is open season except what we have written a particular law about — which winds up being impossible to keep up with."

Though federal law is not aggressively addressing the collection and use of personal data in the U.S., McGeveran and Konnoth both told me there are states that are taking steps to tackle the issue. Two such examples include California, with the recently passed California Consumer Privacy Act — currently the strictest privacy law in the country — and Colorado, with its recently strengthened Consumer Data Protection Law.

"All the countries in Europe and Asia have a different model (for protecting personal information) than the United States," said McGeveran. "In the U.S., we call this area of law 'privacy law,' but all these other countries call it 'data protection law.' And that's not just a difference in name, it's a difference in attitude.

"Those other systems don't start with the assumption you should have nothing to hide, and the only reason you would want to keep information private is because it's a secret."

When I asked Konnoth if protected entities could sell or share individuals' personal medical data if it was made anonymous, he replied, "They can absolutely sell your information, as long as they strip your record of 18 identifiers. This gets them to HIPAA safe harbor. …. And once data is anonymized, it's no longer protected — even if it comes from a company in the medical space."

This then begged the question: Is it possible for anonymized data to be de-anonymized?

According to an April 2017 Georgetown Law Technology Review post, the answer is yes: "Only a very small amount of data is needed to uniquely identify an individual. Sixty three percent of the population can be uniquely identified by the combination of their gender, date of birth, and ZIP code alone."

And the proliferation of publicly available online data combined with highly sophisticated computer algorithms can now transform previously "scrubbed" data into records that are easily traced back to their original, anonymous owners.

"It's very hard for consumers to know what to do to protect themselves," said Konnoth. "This is an area that requires stronger legislation and enforcement."

He added this optimistic observation, however: "Once you're subject to California and Europe, your practices will generally conform to those two behemoths wherever you are."

Need help? Send your questions, complaints and column ideas to HelpSquad@pioneerlocal.com.

Cathy Cunningham is a freelance columnist.