Companies should rethink data collection

October 19 2015

Last week, the European Court of Justice struck down a 15-year-old agreement that allowed companies to move European citizens' personal data to servers in the United States. The so-called Safe Harbor agreement had made it possible for American companies to skirt European data privacy laws, many of which are stricter than U.S. laws.

It's not entirely clear yet what the implications will be for U.S. companies like Google, Amazon and others, but Brown computer scientist Anna Lysyanskaya says now might be a good time for companies rethink how they handle personal data. One obvious solution, she says, is to avoid collecting personal data in first place. Lysyanskaya talked about this and other cybersecurity issues earlier this week at the Grace Hopper conference.

"There are cryptographic options out there that allow companies to interact with customers without collecting personal information," Lysyanskaya said. "If they never collect the data, they don't have to worry about how to protect it."

Lysyanskaya has spent years developing one such technique, known as anonymous credentials. In general, when people sign up for online products like newspaper subscriptions or streaming services, they create a profile with information that identifies who they are—names, birthdates, credit card numbers, etc. The service provider uses that information, along with a username and password, to verify that a person is an authorized user of the service.

Anonymous credentials, on the other hand, take personal information out of the picture.

"It's a means by which a provider becomes convinced that a user is authorized without ever knowing the user's actual identity," Lysyanskaya said. "All the provider knows is that you're authorized; they know nothing else about you."

It works through what's known as a zero-knowledge proof. Through an algorithm, the user supplies encrypted credentials—a kind of cryptographic puzzle—to the service provider. An algorithm on the provider's side asks a series of questions that prove whether or not the user knows how to solve the puzzle. Once the algorithm is convinced that the user can solve the puzzle, it grants access without ever identifying who the user is.

Technologies like this could keep companies from running afoul of data privacy laws in light of the European Court ruling, Lysyanskaya says. "They can't get into trouble for data they never collect."

Such technologies haven't been widely used to this point, but are readily available. IBM Research, for example, offers system called Identity Mixer, which is based on an algorithm Lysyanskaya developed. With a bit of tailoring, anonymous credentials can be used in a wide variety of settings. "Anything you can do with non-anonymous credentials, you can do anonymously today," Lysyanskaya said.

Provided by Brown University