Prof Warns of Risks on Social Network Sites

October 7 2009

Dr. Murat Kantarcioglu

(PhysOrg.com) -- The data that can be easily extracted from people's online social networking activities could be either a blessing or a curse, says a UT Dallas researcher.

On the one hand, an analysis of people's interactions could improve public policy, helping city planners, for example, determine optimal locations for public health clinics. But on the other hand, you could have your identity stolen and your savings account wiped out after sharing seemingly innocuous details about yourself.

These are the sorts of things Dr. Murat Kantarcioglu is exploring.

In the early stages of his research, he's asking questions such as whether details of your Facebook user profile and friendship links can be used to

accurately predict your political affiliation. (Yes, according to his results.) Another question is whether a prospective employer could use your information to try to predict whether you would make a good employee. And if so and you object to that, what could you do to protect yourself?

“Definitely we lose some of our privacy by participating in social-networking sites like Facebook,” said Kantarcioglu, an assistant professor of computer science. “And powerful data analysis tools definitely allow people to infer things you may wish to keep private. But just what private information can be inferred from the information you divulge? That’s one of the things we’re looking at right now.”

Another basic question is how much information can be gathered without ever impinging on people’s privacy?

“Social network analysis is possible in many ways,” he said. “You can analyze e-mail traffic among people in an organization, for example, and without actually reading any of the e-mails themselves learn something from the patterns of the relationships among employees, including the centers of influence in an organization.”

And the potential benefits of social-network analysis are hard to ignore.

Studying social networks of romantic relationships among high school or college students, for example, might reveal who’s at risk of contracting a sexually transmitted disease, helping drive public health efforts. Social-networking analysis can depict such relationships in a graphic that previously would have required months of research.

“Now it’s easy to just write a program to extract the social network information you’re interested in,” said Kantarcioglu, who is also director of the Data Security and Privacy Lab in the Erik Jonsson School of

Engineering and Computer Science at UT Dallas.

“The trick is how to get the advantages without compromising privacy,” he added. “That’s what we’re working on here.”

But companies with their own interests are increasingly asking themselves what they can do with social-networking information, he said.

“What kind of analysis or data mining can they do to get information about, say, purchasing preferences?” he asked. “What conclusions or suppositions about you can they arrive at based on who your friends are and what they know about those friends?”

People are sharing vast amounts of personal information about themselves, for better or worse, he said.

“It’s easy now to link together credit card purchases with Facebook data, geographic information, etc.,” he said. “No one that we know of at this point is combining it all, but I think eventually they will.”

People may ask, What do I have to hide? But Kantarcioglu points out that by revealing your birth date and your hometown, others can infer up to five digits of your Social Security number, putting them just four digits away from identity theft.

Or what if something you revealed casually on a social-networking site caused your insurance company to raise your premium?

“The safest thing is to put as little information as possible out there,” he said.

If you put it out there, he added, it will be there forever. He suggests

people ask themselves, Would I have a problem if everyone were to see this?

“Techniques can be developed to do useful analysis that would benefit city planning and public health and other public policy issues,” he said. “But how do you extract that useful information from the data without sacrificing privacy? I think we can both collect the information and protect privacy if we try harder.”

Protecting Your Privacy on Social Networking Sites

A few things to keep in mind when posting information about yourself.

• The first five digits of your Social Security number are derived from your birth date and your hometown. So if you post your birth date and hometown — and many people do — you could potentially be revealing over half of your Social Security number.

• Make sure your privacy settings on social networking sites are set to provide you with the level of privacy you want. “Many people are not using the privacy settings to their fullest,” Dr. Kantarcioglu said.

• Don’t post any pictures that you wouldn’t want the whole world to see.

The information on Facebook and other social-networking sites isn’t public, but Murat Kantarcioglu believes it’s wisest to think of it as being at risk of becoming public.

Provided by University of Texas at Dallas (news : web)