



The problem with privacy? Security

SECTOR 2010 In a room full of security pros, Tracy Ann Kosa argues that privacy issues are "all security's fault"

By: Dave Webb

ComputerWorld Canada (27 Oct 2010)

Mark Zuckerberg of Facebook. Scott McNeilly of Sun Microsystems. Eric Schmidt of Google. They've all proclaimed the death of privacy. Notice what they have in common? Tracy Ann Kosa does.

"They all have a direct financial benefit from the death of privacy," the privacy impact assessment specialist with the government of Ontario during her keynote at the SecTor 2010 security education conference in Toronto Tuesday.

In a room full of IT security pros, her basic premise – "This is all security's fault" – could have gotten a cooler reception. Kosa preaches a fundamental re-think of the relationship between security and privacy: "When we start talking about security, it's too late to talk about privacy."

Kosa cited Gwynne Dyer's Grand Historical Theory of Technology: Until 5,000 years ago, we were hunter-gatherers, and we all had a say around the campfire for our groups of about 100 people; decision-making was communal. The advent of agriculture, allowing settlements of 10,000 or 20,000, demanded a hierarchy to function, and with that came "all the wonderful things that come with hierarchy" – tyranny, oppression and dictatorship. The technology age, beginning with the newspaper, gave the people their voice back, seeded the age of revolution, and restored some egalitarianism.

"Technology has the capacity to return us to where we were," Kosa said.

But throw the profit motive into the personal information equation, and we get a hierarchy again, as some get rich and some get poor.

"Personal information is not just an asset, it's a product," Kosa said. "Privacy ... has become an obstacle to selling that information."

Kosa notes that in retail privacy breaches, the majority of firms, on their last Payment Card Industry Data Security Standard (PCI DSS) audit prior to the breach, reported 100 per cent compliance. If a standard doesn't work, asked Kosa, why would we use it?

In response to ever-more-complex data collection, an ever-more-complex infrastructure is put into place to protect that data. But when the system fails, it's the user that takes the blame, not the infrastructure, said Kosa.

As an example of an excessively complex data collection system, Kosa points to the U.S. social security system. Social security numbers are issued at birth in the U.S. But those SSNs can be used to apply for credit by identity thieves before the SSN-holder has turned 18 and is legally entitled to credit. The solution? Another database to track SSN-holders who haven't reached the age of majority, which must be consulted (and often isn't) by credit-granting organizations, and which is itself vulnerable to exploitation.

Wouldn't it make more sense, Kosa asked, to clear credit records when the SSN-holder turns 18? When profit is thrown into the equation, security and privacy butt heads.

Computer sciences' security-first approach to privacy ignores the fact that we could have created a system that didn't collect the information in the first place. We have to start asking whether it's necessary to collect personally identifiable information to provide the product or service we're providing, Kosa said.

"When we start talking about security, it's too late to talk about privacy," she said.

On the other hand, the behavioural sciences don't have a stellar track record when it comes to ensuring privacy, either, she said. Approaches that try to influence people's decisions about privacy through cost-benefit analyses or quantified values of privacy don't work, she said, because privacy decisions are completely unstable" and "100 per cent contextual," she said.

Copyright © 2010
ITworldcanada.com

[web analytics](#)