Print

Wednesday, July 28, 2010 3:19 PM EDT

Online privacy: Is there any?

By Joseph Picard

On April 1, 2010 - April Fools Day - the British games retailer, GameStation, obtained the legal rights to about 7,500 immortal souls.

GameStation pulled off the Mephistophelean feat by adding a clause to its online privacy policy and conditions for using the GameStation website that said, unless the user opts out, the company takes possession of the user's "Immortal Soul." The company was making the point that few people read those conditions before accepting them. About 88 percent of users relinquished their souls that day.

Jon Leibowitz, chairman of the Federal Trade Commission, retold the story Tuesday to the Senate Commerce, Science and Transportation Committee's hearings on "Consumer Online Privacy."

"Most consumers believe a privacy policy protects their privacy," Leibowitz said. "In fact, a privacy policy delineates their rights and the lack thereof. Privacy policies do not generally protect consumers, and consumers do not generally read them."

Sen. Jay Rockefeller, D-WV, the committee chairman, ask if the American consumers who go online "fully understand and appreciate what information is being collected about them, and whether or not they are empowered to stop certain practices from taking place?"

Misunderstood privacy policies, the ability of users to opt out of data collection and the tracking of users for advertising purposes were among the Senators' main concerns.

Sen. Byron Dorgan, D-ND, called the practice of Internet tracking "snooping."

"If you went to" a shopping mall "and stopped at Chipolte's, then Nordstrom's...then a jewelry store, then, maybe, Annie's Pretzels, then a bookstore where you bought *Rolling Stone*, *Better Homes and Gardens* and *How to Make a Nuclear Weapon*," Dorgan said.

"And someone followed you every step of the way, just over your shoulder, making copious notes on your behavior. Anyone would find that unbelievable," he continued. "They'd say who are you to be following me around taking notes? Yet that sort of thing is happening every day to people using the Internet."

The questions, Dorgan said, are who is gathering this information and how is it being used?

Representatives from Apple, Facebook and Google each said that their companies conscientiously serve their users and protect their privacy.

"Location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services," said Guy "Bud" Tribble, Apple's vice president for Software Technology.

Tribble added that Apple's privacy policy statement is "in easy-to-read language" and available by link on every page of Apple's website.

Bret Taylor, chief technology officer for Facebook, said the company connects "advertisers with people in a way that is unobtrusive."

"We do this without selling user information to advertisers or giving advertisers access to personal information," he said.

Alma Whitten, Google's privacy chief, emphasized that "we do not sell our users' personal information."

She then explained that Google launched Internet-based advertising in March, 2009. She said Google shows ads based on the content of the page the user is viewing as well as ads "based on interest categories" the user "might find useful."

But Joseph Turow, professor at the University of Pennsylvania's Annenberg School of Communication, said that online companies do not sufficiently regulate themselves and that educating the public to their choices regarding online data collection is also not enough to stop abuses of privacy.

"When companies track people without their knowledge, sell their data without their knowledge or permission, and then decide whether they are, in the words of the industry, targets or waste, we have a social problem," Turow said.

Turow said "online advertising exchanges, owned by Google, Yahoo, Microsoft, Interpublic and other major players, allow for the auction of individuals with particular characteristics."

"It is now possible to buy the right to deliver an ad to a person with specific characteristics at the precise moment that the person loads a web page," Turow said.

Turow debunked companies' claims to protecting users' anonymity.

"If a company can follow your behavior in the digital environment -- and that potentially includes the mobile phone and your television set -- its claim that you are anonymous is meaningless," he said. "That is particularly true when firms intermittently add offline information to the online data and then simply strip the name and address to make it 'anonymous.'"

Turow said eXelate, a targeting exchange, "determines consumer's age, sex, ethnicity, marital status, and profession by partnering with websites to scour website registration data."

The firm Rapleaf, Turow said, boasts of having "data on 900+ million records, 400+ million consumers, and 52+ billion friend connections," and sells "the ability to reach those individual cookies."

"A company called Medicx Media Solutions links HIPAA certified medical and pharmacy insurance claims data for tens of millions of Americans to information about them from information suppliers such as Experian, as well as from health surveys people fill out," he said. "Even though Medicx cannot tie the data to particular individuals, it does retain an ability to connect the medical, pharmacy, and survey findings to ZIP+4 postal clusters of 3 to 8 homes."

Turow called upon Congress to step in and help consumers with legislation.

"One path is to limit the extensiveness of data or clusters of data that a digital advertiser can keep about an individual or household," he said.

But Jim Harper, director of Information Policy Studies at the Cato Institute, said history shows that government interference in privacy issues does not bear fruit.

"Over decades, a batch of policies referred to as 'fair information practices' have failed to take hold because of their complexity and internal inconsistencies," Harper said. "Even modest regulation like mandated privacy notices have not produced meaningful improvements in privacy."

Harper said the fact that consumers do not, in general, read privacy policy notices indicates that "they either do not consider privacy much of the time, or they value other things more than privacy when they interact online."

Harper said that "privacy is subjective," and therefore, "government regulation in the name of privacy can be based only on guesses about what privacy should look like."

Harper said the proper approach is consumer education about what they reveal when they interact online.

He said all the "fretting" about Internet behavioral advertising could be minimized if people simply learned to use controls already provided by Internet companies.

"The remedy for most of it is so utterly simple: exercising control over the cookies in one's browser," Harper said.

Fran Maier, founder and president of TRUSTe, a San Francisco-based Internet privacy services provider for businesses and consumers, was not at the hearing, but said in a phone interview that consumer online privacy depends on transparency - that is, letting consumers know where their data is going; giving consumers a clear choice on whether, and how much, they may want to participate in an activity; and in holding online companies, as well as offline companies, accountable for what they do with consumers' data.

"Many companies online are innovating very quickly," she said." It is not surprising that these issues arise. It is the nature of the beast. Legislation can help, but legislation is often unable to keep up with the pace of innovation."

Maier said that to protect consumer privacy while still offering the benefits of the Internet requires a coordinated approach that includes technology, self-regulation, consumer education and legislation.

"But we should take an approach that does not make up people's minds for them - we know that people do not want others making up their minds for them," Maier said.

Apple is one of TRUSTe's clients.

The FTC's Leibowitz said the Commission could use more clout in making companies adhere to practices aimed at protecting consumer privacy.

He said the FTC has unsuccessfully sought legislation in the past to ensure that businesses provide notice of what information they collect from consumers and how they use it; give consumers choices about how information collected from them may be used; allow consumers access to data collected about them; and ensure the security of the information they collect.

Leibowitz said there are many examples of companies not keeping their word to their users.

The FTC has "brought law enforcement actions to hold companies accountable for their privacy statements and practices," he said.

In 1999, the FTC went after GeoCities for misrepresenting "the purposes for which it was collecting personal information from both children and adults. In 2000, the Commission challenged a website's attempts to sell personal customer information, despite the representation in its privacy policy that such information would never be disclosed to a third party."

Leibowitz also cited FTC cases against Microsoft, ChoicePoint, CVS, LexisNexis and Twitter, for the alleged failure to comply with posted privacy policies, dispose of data safely, and take reasonable steps to guard against sharing customer data with unauthorized third parties.

"In each case, the Commission obtained significant relief, including requiring the companies to implement a comprehensive information security program and obtain regular third-party assessments of the effectiveness of that program," he said.

The FTC has also won judgments against website operators that collect information from children without first obtaining their parents' consent, securing over $3.2 million in civil penalties, Leibowitz said.