Cloud computing user privacy in serious need of reform, scholars say

June 11 2013

University of Illinois law professor Jay P. Kesan says the current "non-negotiable approach" to user privacy is in need of serious revision, especially with the increased popularity of web-based software that shares information via cloud computing. Credit: L. Brian Stauffer

When Web surfers sign up for a new online service or download a Web application for their smartphone or tablet, the service typically requires them to click a seemingly innocuous box and accept the company's terms

of service and privacy policy. But agreeing to terms without reading them beforehand can adversely affect a user's legal rights, says a new paper by a University of Illinois expert in technology and legal issues.

Law professor Jay P. Kesan says the current "non-negotiable approach" to user privacy is in need of serious revision, especially with the increased popularity of Web-based software that shares information through cloud computing.

In a recently published paper in the *Washington and Lee Law Review*, Kesan and co-authors Carol M. Hayes, a research associate in the College of Law, and Masooda N. Bashir, the assistant director of the Social Trust Initiatives at the U. of I.'s Information Trust Institute, propose creating a legal framework that would require companies to provide baseline protections for personal information while also taking steps to enhance users' control over their own data.

"Our goal with this piece is to raise awareness of the privacy of online information, which is something that people seem to care about a lot more once they actually know what companies are doing with their personal information and data," said Kesan, the H. Ross & Helen Workman Research Scholar in the College of Law.

With so many of our daily activities now taking place "in the cloud," Kesan cautions it's still perfectly acceptable for users to give away personal information to online services – so long as they're comfortable with allowing companies to snoop, aggregate and data mine their online habits.

"If you think it's a fair trade to receive an email service in exchange for letting a company track what Web pages you visit and show you relevant advertisements, by all means, you should continue to do so," Kesan said. "But there are always security risks involved when information is stored,

electronically or not. Users must weigh the advantages and disadvantages of the available options."

In the article, the scholars analyzed and categorized terms-of-service agreements and privacy policies of several major cloud-based services to assess the state of user privacy. Their analysis shows that providers all take similar approaches to user privacy, in that providers were consistently more detailed when describing the user's obligations to the provider than when describing the provider's obligations to the user.

"It's the provider who sets the terms, knows the terms inside and out, and ultimately benefits from the terms," Kesan said. "But because these obligations are usually in the form of an 'adhesion contract,' and only one party has bargaining power, the consumer does not have the ability to counter with new terms, ones that could increase their benefits."

In the article, the authors describe personal information as being akin to online currency.

"You're essentially bartering with a lot of these online service providers," Kesan said. "You give them access to your information, and they aggregate this information to create a profile of you as a consumer. Most of these companies do not outright sell your information unless you tell them that it's OK to do so. But by giving them your information in exchange for the service, you have essentially engaged in bartering. And what we want is for people to recognize that this is a business exchange."

And while the user gives the service what they want, the service also imposes additional terms that the user probably doesn't read.

"So not only are these one-sided agreements that are designed to benefit the provider of the service, the consumer who clicks 'I agree' also is woefully under-informed about what it is that they just agreed to," Kesan

said.

"It's very difficult to weigh the advantages and disadvantages and then make an informed decision, if you don't know what's actually going on. All of this additional information means that their advertising space is more valuable. But when consumers are not informed, they're bartering their goods in exchange for one identified item and one box with unknown contents."

That asymmetry, combined with these terms' non-negotiable nature, led the authors to conclude that there's a real need for "data control" in the cloud, Kesan said.

According to the authors, they define data control as consisting of two parts: data withdrawal, which is the ability to withdraw data and require a service provider to stop using or storing the user's information; and data mobility, which is the ability to move data to a new location without being locked into a particular provider.

"We want consumers to feel confident in their decisions, and to know and understand what they have agreed to," Kesan said. "We want them to have the ability to make a meaningful choice between cloud service providers, even if they've already chosen one, and they should be able to easily migrate their information if a better service becomes available.

"Second, we believe that consumers should have the option of withdrawing their data from use by marketers. We realize that service providers may have created metadata from information that can't be withdrawn. But the value of that metadata will reduce with time, if the consumer chooses to withdraw their existing data."

According to Kesan, the ultimate goal of the paper was to apply established law and privacy theories to services in the cloud and set forth

a model for the protection of information privacy that recognizes the importance of informed and empowered users.

Kesan also believes that a "light-touch regulatory intervention" – that is, something similar to when the Federal Communications Commission required cellphone carriers to allow users to port their phone numbers to different carriers – would be beneficial.

"The cellphone providers initially opposed allowing customers to transfer, or port, their cellphone numbers from one provider to another, claiming that it would be too costly for carriers, and would not actually provide a benefit to the customers," he said.

In 2006, three years after wireless carriers were required to make cellphone numbers portable, the FCC concluded that number porting had a positive impact on service quality because of the need that it created for companies to focus on customer retention, Kesan said.

"We believe that this approach would also work with the problem of how to change cloud service providers, without the customer being excessively burdened by the change," he said.

When policymakers start to have this conversation with businesses, they need to emphasize how much businesses stand to gain by adopting policies that protect consumers, Kesan said.

"Consumers need to have some baseline set of rights to make this market of cloud services work more efficiently," he said. "When the market works more efficiently, we think businesses will see benefits."

More information: The article, "Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency," is available online.