Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

International Standard Could Reshape Cloud Privacy

Law360, New York (October 21, 2014, 10:05 AM ET) --

Lindsey Tonsager

The work of international standards bodies can effectively discourage the adoption of patchwork, and potentially contradictory, regulation in multiple jurisdictions around the world. By developing voluntary global standards that are widely supported across a particular industry, international standards bodies can address some of the most important public policy issues of the day.

For example, the International Standards Organization ("ISO") and the International Electrotechnical Commission ("IEC") have developed a number of information security standards, such as ISO/IEC 27001 and ISO/IEC 27002, that identify technical controls for organizations to protect the security of personally identifiable information. More specifically, ISO/IEC 27018 sets forth technical controls and techniques that are tailored to protecting personally identifiable information maintained by cloud service providers, such as Amazon Web Services, Microsoft Office 365 and Google Apps for Work, that process such information.

Because the standards-setting process tends to be supported primarily by engineers and other technical consultants, the resulting standards often are perceived to be workable, practical measures that take into account the capabilities of existing technology. At the same time, however, international standards are almost always highly technical documents. They tend not to outline broad statements of policy or legal frameworks.

But this summer the ISO and IEC took the bold step of adopting a new voluntary international standard that proposes a broad policy framework for protecting the privacy of personally identifiable information processed in the cloud. Specifically, to achieve ISO/IEC 27018 certification, cloud service providers must (among other things):

- Be transparent about their practices. Cloud service providers must notify the businesses and other customers that contract for their cloud services of (1) the countries where personally identifiable information may be stored, (2) the identities of any sub-contractors retained to help process such information, and (3) the possible locations where such information may be processed (including by sub-contractors).

- Not use customer's personally identifiable information for the cloud service provider's own independent purposes, without the customer's express consent. Cloud service providers must process personally identifiable information only in accordance with the customer's instructions and cannot use such information for marketing, targeted advertising, or data analytics without express consent from the customer. Consent cannot be a condition for receiving the cloud service.

- Help customers respond to individual end user requests for access to personally identifiable information. A cloud service provider must offer tools to help their customers comply with their obligations to individual end users, including allowing end users to access, correct, or erase their personally identifiable information.

- Help customers notify individual end users and others as necessary in the event of a data breach. Cloud service providers must notify their customers of data breaches "promptly" and help these customers comply with their data breach notification requirements. In addition, cloud service providers must record specific information about data security incidents, including the type, timing, consequences, and any remedial steps taken.

- Not disclose personally identifiable information to law enforcement authorities unless legally required to do so. Cloud service providers must refuse law enforcement requests to disclose personally identifiable information unless required by law. If disclosure is required, the cloud service provider must notify the affected customer, unless prohibited from doing so by law.

- Enable the customer to switch cloud service providers. Cloud service providers must implement a policy for the return, transfer or disposal of personally identifiable information entrusted to them by their customers. The policy must specify the period for retaining such information following the termination of the agreement.

- Undergo periodic information security audits by an independent third party.

A number of leading cloud service providers in the United States and Europe already have announced plans to certify under the standard. And because ISO/IEC 27018 is the first international standard to focus on privacy in the cloud and provides an auditable policy framework for privacy compliance, it could significantly shape cloud services around the globe.

ISO/IEC 27018 also provides a helpful benchmarking tool for legal practitioners engaged in due diligence for new cloud services. Specifically, businesses and other customers negotiating cloud service agreements should ask the following three questions:

1. Does the cloud service provider have an ISO/IEC 27018 certification? Customers can verify whether the cloud service provider complies with the standard by checking to see if it has a certificate of conformity from an independent certification body. Most certification bodies have a process on their websites for checking the validity of a certificate.

2. If the cloud service provider does not have an ISO/IEC 27018 certification, will it agree to a third-party audit against the ISO/IEC 27018 controls? Because the ISO/IEC 27018 standard is designed to provide

auditable controls, customers can use an independent third-party audit to identify whether there are any gaps in how an uncertified cloud service provider protects personally identifiable information.

3. Will the cloud service provider agree to comply with industry best practices, including ISO/IEC 27018? As the first privacy-specific international standard for cloud services, ISO/IEC 27018 catalogues current best practices for cloud service providers to comply with data protection laws around the world and to protect end-users' personally identifiable information.

—By Lindsey Tonsager, Covington & Burling LLP

Lindsey Tonsager is an associate in the Washington, D.C., office of Covington & Burling.