Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

Volume 13, Number 6 June 2013

The Expanding Reach of U.S. Laws Protecting Health Information and Children's Information

By Christine Lyon, Julie O'Neill, and Andrew Serwin, of Morrison & Foerster LLP. Christine Lyon is a member of the World Data Protection Report Editorial Board.

The United States is expanding two key federal privacy laws to cover a broader range of websites, online services, and cloud-based services. The first is the Health Insurance Portability and Accountability Act ("HIPAA"), which originally applied only to health care entities but now will apply equally to service providers storing protected health information on behalf of such entities. The second is the Children's Online Privacy Protection Act ("COPPA"), which now extends to more websites and online activities that collect information from children under the age of 13.

This article describes the expanded coverage of HIPAA and COPPA and the types of businesses that may find themselves swept into these laws for the first time.

HIPAA Reaches for the Cloud

HIPAA is the primary U.S. federal law governing the privacy and security of health information. HIPAA imposes extensive privacy and data security obligations on health care entities and, increasingly, on their service providers as well.

The new changes to HIPAA mean that companies that provide data support or storage may now fall within the expanded definition of a business associate. According to HHS, this is true even if the company that is offering storage or other support does not *actually view* the protected health information.

HIPAA's Expansion to Business Associates

Initially, HIPAA applied only to covered entities in the health care sector: health care providers, health plans, and health care clearinghouses. HIPAA required these covered entities to impose rigorous privacy and data security obligations on their "business associates"—*i.e.*, companies processing protected health information (or "PHI") on their behalf—but HIPAA did not apply directly to business associates.

The first major expansion of HIPAA occurred in 2009,

when the Health Information for Economic and Clinical Health Act ("HITECH Act") extended HIPAA's privacy and data security obligations to apply directly to business associates. However, under the definition of "business associate" in effect at that time, many companies assumed that business associate status was limited to companies that actively processed PHI for covered entities. In particular, cloud providers often asserted that they would not be deemed a "business associate" merely because a covered entity happened to store PHI in their cloud.

HIPAA's Expansion to Passive Data Storage Services

In January of this year, the Department of Health and Human Services ("HHS") issued new regulations indicating the contrary: that mere storage of PHI now may be sufficient to create business associate status. Now, the definition of a "business associate" includes subcontractors that create, receive, maintain, or transmit PHI on behalf of a covered entity or even another business associate (*see WDPR, January 2013, page 29*).

HHS has confirmed that the new regulations create downstream liability for subcontractors that did not exist before. These regulations became effective on March 26, 2013, and covered entities and business associates are required to achieve compliance by September 23, 2013.

HHS further maintains that a technology provider that has the ability to access PHI is likely to be considered a business associate, even if the provider may never intend to access PHI. HHS acknowledged that where a company acts as a "mere conduit"—such as a telecommunications company, internet service provider, or courier service—it is not a business associate. However, when the provider stores or maintains data, HHS emphasized that provider would be considered a business associate.

The question of whether a provider is a business associate requires a fact-specific analysis based upon the nature of the services provided and the extent to which the provider needs access to PHI to provide services to the covered entity. There is no knowledge component to the determination of whether a company is acting as a business associate: A company may be found to be a business associate without even knowing it.

These changes mean that companies that provide data support or storage may now fall within the expanded definition of a business associate. According to HHS, this is true even if the company that is offering storage or other support does not *actually view* the PHI. As a result, a software company that hosts software or data containing PHI on its own server, or accesses PHI when troubleshooting the software function, is considered a business associate.

The expanded regulation also affects data storage providers, including cloud storage providers, to the extent they store PHI on behalf of a covered entity or business associate, unless the cloud storage provider falls within the narrow "conduit" exception.

Practical Consequences

Before the September 2013 enforcement deadline, covered entities and existing business associates should 1) identify any entities that create, receive, transmit, or maintain PHI on their behalf but have not executed a business associate agreement, and 2) assess whether they now need to require any of those entities to enter into a business associate or similar agreement.

Meanwhile, companies providing cloud or data storage services should assess whether they may become subject to HIPAA as business associates, under this revised definition. If so, they will need to address not only their own compliance with HIPAA's privacy and security rules (such as conducting a risk analysis and implementing HIPAA-compliant security procedures), but also the need to ensure HIPAA compliance by any subcontractors that may be handling the PHI on their behalf.

COPPA Pushes the Boundaries of Personal Information

Like HIPAA, COPPA has been expanded to reach a broader range of companies.

COPPA restricts the collection of personal information from children under the age of 13 through a website, application, or other online service (each, an "Online Service").[1] For example, COPPA requires Online Services to obtain verifiable parental consent before collecting personal information from children, to provide the parent with a prescribed form of notice when seeking consent, and to allow parents to access and review the personal information collected from their children, as well as to revoke consent previously provided and/or to request that the personal information be deleted. Companies that become subject to COPPA often must implement significant changes to their data collection and handling practices.

COPPA applies to operators of Online Services that are directed toward children or that knowingly collect personal information from children. However, COPPA is not limited to Online Services that are overtly directed toward children. A revised COPPA rule that will take effect on July 1, 2013,[2] may extend COPPA obligations to companies that do not view themselves as operating child-oriented Online Services (*see WDPR, January 2013, page 30*).

A revised COPPA rule that will take effect on July 1, 2013, may extend COPPA obligations to companies that do not view themselves as operating child-oriented Online Services.

The revised rule also expands COPPA's coverage by broadening its definition of "personal information," thus covering more types of online data collection. For example:

   ISSN 1473-3579

- **Third-party services that collect personal information through an Online Service subject to COPPA**: COPPA now expressly covers third-party services (such as advertising networks or social plug-ins) that collect personal information on or through a COPPA-regulated Online Service. The operator of the Online Service is strictly liable for that third party's compliance with COPPA, while the third party becomes liable under COPPA only if the third party has actual knowledge that it is collecting personal information through a child-directed Online Service or from a child. Despite the actual knowledge standard, this expansion of COPPA increases the stakes for third parties collecting information through Online Services that may be subject to COPPA.
- **Online Services involved in online behavioral advertising**: The new COPPA rule contains an unusually broad (by U.S. standards) definition of "personal information" that includes a "persistent identifier."[3] However, the collection of a persistent identifier does not trigger COPPA's obligation to obtain verifiable parental consent if such collection is strictly necessary to support the internal operations of the Online Service.[4] Expressly not included within the definition of "support for the internal operations" of the Online Service are activities such as retargeting and other online behavioral advertising—for which, accordingly, verifiable parental consent would be required. This change in the rule could sweep in child-oriented websites or online services that do not view themselves as collecting personal information, but which do collect persistent identifiers to display targeted advertising. The revised rule also newly defines "personal information" to include a child's image or voice (*e.g.*, in a photo, video, or audio file), geolocation information at least equivalent to street name plus city or town, or screen or user name when it is sufficient to permit the online contacting of the child. Therefore, operators of child-directed Online Services should assess whether their information collection practices may capture more "personal information" than they intend.

The revised rule also expands COPPA's coverage by broadening its definition of "personal information," thus covering more types of online data collection.

Unlike HIPAA, COPPA obligations do not directly apply to service providers handling covered data on behalf of a regulated entity. However, the new COPPA regulations do require covered operators to pass through stricter data security obligations to service providers. They require the operator to take reasonable steps to release children's personal information only to service providers that are capable of maintaining its confidentiality, security, and integrity, and that provide assurances that they will do so. Accordingly, companies that provide data processing or storage services for COPPA-regulated Online Services may encounter greater pressure from customers to provide written assurances about their data security measures.

Practical Consequences

In light of the revised rule, an Online Service that is directed to children or that has actual knowledge that it collects personal information from children (for example, because it collects date of birth or age) should review how "personal information" is collected through it, in order to determine whether the revised rule's broader definition affects its compliance obligations.

In particular, an Online Service should review whether it collects geolocation information, a screen or user name that permits online contact, or photographs, videos, or audio files.

It should also consider its use of persistent identifiers, to establish whether any such use requires verifiable parental consent.

Moreover, an Online Service should identify any third parties that collect personal information on or through the service (such as an advertising network or social plug-in), to assess their compliance obligations and the service's own attendant exposure.

Conclusion

The recent expansions of HIPAA and COPPA reflect growing concern in the United States about protecting sensitive information, such as health information and children's information, especially in the online context. In particular, companies handling health information or children's information should assess the degree to which these changes to HIPAA and COPPA may affect their privacy and data security practices.

NOTES

[1] For purposes of this discussion, "children" refers to children under 13 years of age.

[2] *See* http://www.ftc.gov/os/fedreg/2013/01/130117coppa.pdf. The revised rule will be codified at 16 C.F.R. Part 312.

[3] A "persistent identifier" is an identifier "that can be used to recognize a user over time and across different websites or online services." It includes, for example, "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier." 16 C.F.R. § 312.2 (definition of "personal information").

[4] 16 C.F.R. § 312.5(c)(7).

Christine Lyon is a Partner in Morrison & Foerster LLP's Palo Alto, California, office, and a member of the World Data Protection Report Editorial Board. She may be contacted at clyon@mofo.com. Julie O'Neill is Of Counsel in the law firm's Washington, D.C., office. She may be contacted at joneill@mofo.com. Andrew Serwin is a Partner in the firm's San Diego, California, office. He may be contacted at aserwin@mofo.com.