Developments in Cyber Security and Privacy Law Continue to Affect Technology Companies

by Jonathan S. Storper

Several new California laws have been enacted in the last year and the SEC is also getting in the act regarding cyber security risks.

A new personal information privacy law went into effect in California this year. If a person or business is the source of a breach of security, the business must provide identity theft protection for no less than twelve (12) months following the breach to those affected in addition to disclosing the security breach. California also put into effect this year prohibitions on certain advertising to minors. California website operators are now prohibited from advertising a product or service to a minor in any of nineteen (19) categories outlined in the new law. Categories include: alcohol, firearms, ammunition, spray paint, BB guns, fireworks, tobacco, tanning devices, diet pills, tattoos, lottery tickets, drug paraphernalia, electronic cigarettes and obscene matters among other things. If a website operator uses an advertising service, the operator can stay in compliance with that statute as long as the advertising service is advised that the site is directed to minors and the advertising service puts specific measures into place to prevent such advertising.

California also instituted an "internet eraser law" which requires web hosting companies and other entities hosting content of others to implement new take-down options for minors. Anyone under the age of eighteen (18) who is a registered user of a website may remove or request removal of content posted by that minor. The website operator also has to provide notice that the minor has such a right, with clear instructions as to how to accomplish the removal, along with advice that such removal does not necessarily ensure complete or comprehensive removal of content with certain exceptions too detailed to go into here.

Finally, the Securities and Exchange Commission has been thinking about cyber security disclosure regulations. The discussion of a company's "risk factors" in filings should disclose the risk of breaches if they would make an investment in the business material including the potential costs of any breach. While the disclosure depends on the company's particular set of facts and circumstances, disclosures might include a discussion of the company's business or operations that would give rise to cyber security risks, including the risk of breaches that may have

been undetected, a description of relative insurance coverage and a description of incidents that may be material to the company. Although the guidance doesn't have the force of an actual SEC regulation, the agency staff has treated it as such, and has sent comment letters to companies that their disclosures need to be revised to conform to the guidance. Failure to follow such guidance may lead to fines, sanctions and litigation.

For more information, please contact:

Jonathan S. Storper, Partner
415-995-5040
jstorper@hansonbridgett.com