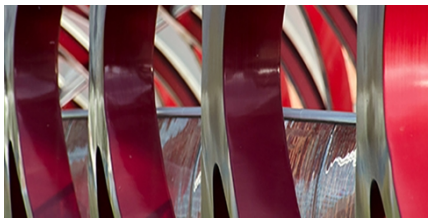
masuda funai



News & Types: Client Advisories

Facebook Privacy Litigation: U.S. Style Data Regulation

4/5/2018

By: Asa W. Markel

Practices: Commercial, Competition & Trade

As the month of March ended, Facebook faced at least sixteen separate lawsuits relating to or spurred by the revelations concerning Cambridge Analytica's access to data from millions of Facebook users. If past data breaches by large American firms is any indication, the avalanche of lawsuits will continue before things get better for Facebook. Yet, Facebook's predicament sheds light on the indirect method of regulating data rights in the United States.

Businesses across the world are bracing for the entry into force in May of the European Union's General Data Protection Regulation (GDPR). The GDPR promises to strengthen the rights of European residents over their data – regulating not only how it is collected from them but how it is handled once it has been collected. More than this, the GDPR imposes restrictions on the transfer of a European resident's data outside the European Union and extends its restrictions to overseas businesses that offer goods and services within Europe. Businesses in Japan have been coping with a similar data regime for nearly a year already. The 2015 amendments to Japan's Personal Information Protection Act (PIPA), took effect in May 2017. The amended PIPA provides Japanese residents with rights similar to those of the GDPR, including the right to have holders of data correct, cease using, or erase that data.

In contrast to the European Union and Japan, the U.S. has no general, nationwide law concerning the protection of personal data. The federal government enforces protections for financial or medical data or information concerning children. Individual American states regulate the handling of most consumer data. Across the U.S., the law generally does not provide individuals with direct control over their data. A person generally cannot insist on editing or deleting data held by a business. However, the business is liable for securing certain types of data, and for reporting data breaches.

And in classic American style, data owners are willing and able to sue businesses that do not safeguard data or fail to honor their stated privacy policies. Government regulators have also been putting increasing pressure on data holders in recent years. Government agencies and private parties were responsible for the avalanches of litigation against Target, Sony, eBay, JP Morgan Chase, PF Chang, Home Depot, and Nieman Marcus, among others, in 2014 and 2015 for data breaches. By 2017, Target in particular was required to pay over $18 million in settlements due to pressure from state regulators.

Eventually, it is possible that the pressure and expense of large scale consumer litigation will force companies in the U.S. market to adopt data handling standards similar to those of European and Japanese businesses,

©2026 Masuda, Funai, Eifert & Mitchell, Ltd. All rights reserved. This publication should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended solely for informational purposes and you should not act or rely upon information contained herein without consulting a lawyer for advice. This publication may constitute Advertising Material.

without the need for government legislation. For American companies that still consider data regulation to be limited to Europe, the next few years may be very expensive ones.

©2026 Masuda, Funai, Eifert & Mitchell, Ltd. All rights reserved. This publication should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended solely for informational purposes and you should not act or rely upon information contained herein without consulting a lawyer for advice. This publication may constitute Advertising Material.