Arnall Golden Gregory LLP
Attorneys at Law

Daily Privacy & Consumer Regulatory Alert

Published by the Privacy and Consumer Regulatory Practice | Washington, DC Office

July 5, 2018

FEDERAL DEVELOPMENTS

Lawmaker Requests More Information Regarding OPM Data Breach

On June 26th, Representative Gerald Connolly (D-VA) sent a letter to the Department of Justice (DOJ) requesting more information regarding the first publicly disclosed case filed by the DOJ involving the illegal use of individuals' personally identifiable information (PII) obtained from the Office of Personnel Management data breach. According to Connolly, the DOJ declined to disclose how the defendants obtained victims' personal information saying that "further details about how the defendants obtained the PII could be useful for the purposes of protecting victims of the breach from further criminal activity." Connolly also requested a meeting with the DOJ to discuss how to "better balance the needs of this particular prosecution and related investigations with breach victims' need to know how their PII is being obtained by criminals."

FTC Enforcement

On July 2nd, the FTC announced a settlement with California-based company, ReadyTech Corporation, for allegedly falsely claiming it was in the process of being certified as complying with the EU-U.S. Privacy Shield agreement. According to the FTC, ReadyTech, which provides online training services, falsely claimed on its website that it is "in the process of certifying that we comply with the U.S.-E.U. Privacy Shield Framework," in violation of the FTC Act. The company initiated an application in October 2016 to the Department of Commerce to participate in the Privacy Shield framework, but failed to complete the necessary steps. Under the settlement, ReadyTech is prohibited from misrepresenting its participation in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization; and must also comply with standard reporting and compliance requirements.

Federal Legislation

The following legislation was recently introduced by Congress:

- Representative Ed Royce (R-CA) introduced H.R. 6192, the "Credit Services Protection Act," which would amend the Credit Repair Organizations Act to facilitate the development of consumer credit services.
- Senator Dianne Feinstein (D-CA) introduced S. 3127, the "Bot Disclosure and Accountability Act of 2018," which would direct the FTC to create a rule to require social media companies to disclose any social media bots on their platform.
- Senator Ben Sasse (R-NE) introduced S. 3182, which would amend the Homeland Security Act of 2002 to provide for the responsibility of the National Cybersecurity and Communications Integration Center to maintain capabilities to identify threats to industrial control systems. Bill text is currently unavailable.

OTHER DEVELOPMENTS

NCC Releases Report Examining Companies' Privacy Settings

On June 27th, the Norwegian Consumer Council (NCC) released a report entitled, "Deceived by Design," highlighting how companies, such as Google and Facebook, use various methods to direct consumers into

consenting to "privacy-invasive" default settings. Various tactics employed by these companies include preselected privacy-intrusive default settings, which are rarely changed by consumers; requiring the disclosure of users' personal information in order to use the service; hiding more privacy-friendly choices; and deceptively claiming the disclosure of personal information and targeted advertising is beneficial to consumers. The report also called into question the companies' compliance with the EU's General Data Protection Regulation. Privacy rights groups in the U.S. and the EU have sent letters to regulators referencing the report and highlighting companies' privacy settings.

Humana Announces Data Breach

On July 2nd, Humana announced that it fell victim to a cyberattack that might have compromised customers' personal information. The cyberattack, which was a cyber spoofing attack, occurred in June 2018 after discovering a significant increase in the number of secure log in errors on its websites from foreign countries. The volume of log in attempts suggested that the hacker had a large database of user IDs and passwords with the intention of identifying valid accounts; however, due to the log in failures Humana believes that the information did not originate from the company. Potentially compromised information included customers' health information, including their claims and provider information, spending account information, and wellness information, including biometric screening information. Humana has blocked the foreign activity and has implemented security controls, such as requiring a password reset, to increase cybersecurity.

This newsletter is published by AGG's Privacy and Consumer Regulatory Practice. For more information, please visit www.agg.com or contact Bob Belair, Kevin Coy, or Montserrat Miller. To subscribe, please email dpcra@agg.com.

©2011-2018. All Rights Reserved. This alert provides a general summary of recent legal developments. It is not intended to be, and should not be relied upon as, legal advice.