Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

South Carolina Enacts Insurance Data Security Act

South Carolina Governor Henry McMaster signed the South Carolina Insurance Data Security Act into law on May 3, 2018. The law, parts of which become effective January 1, 2019, requires entities licensed by the Department of Insurance to, "develop, implement and maintain a comprehensive information security program based on the licensee's Board of Directors, if applicable to require a licensee to monitor the security program and make adjustments if necessary, to provide that the licensee must establish an incident response plan, to require a licensee to submit a statement to the Director of the Department of Insurance annually; to establish certain requirements for a licensee in the event of a cybersecurity event; to require a licensee to notify the Director of certain information in the event of a cybersecurity event; to grant the Director the power and authority to examine and investigate a licensee; to provide that documents, materials, or other information in the control or possession of the Department must be treated as confidential documents under certain circumstances; to provide exemptions from the provisions of this Chapter; to provide penalties for violations; and to authorize the Director to promulgate regulations."

The state's purpose of the Act is "to establish standards for data security and standards for the investigation of and notification to the director of a cybersecurity event applicable to licensees." It does not provide a private right of action for violation of the Act. *Read more*

DATA PRIVACY

California Consumer Privacy Act Likely to Appear on Ballot in November

Businesses are understandably focused this week on the looming effective date for the European Union's General Data Protection Regulation (GDPR). For U.S. businesses, however, a proposed law closer to home would raise similar compliance burdens and create potential litigation risks.

May 24, 2018

FEATURED AUTHORS:

Linn Foster Freedman
Benjamin C. Jensen
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Privacy
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

This November, voters in California will likely be voting whether to pass a ballot initiative, titled “The Consumer Right to Privacy Act of 2018.” Proponents of the Act, which would broadly expand California residents’ rights to their personal data, announced this month that they submitted 625,000 signatures to the California Secretary of State in support of the measure. Assuming the secretary of state certifies that enough signatures are valid (approximately 366,000 signatures are required to qualify), California voters will be in position to directly pass the Act into law. *Read more*

DRONES

Preventing Emerging Threats Act Introduced

Last week, a group of U.S. Senators introduced a bill titled “Preventing Emerging Threats Act of 2018,” which would give the U.S. Department of Homeland Security (DHS) and the Department of Justice (DOJ) the ability to take action against unmanned aircraft systems (UAS or drones) that pose an “unacceptable security risk” to public safety. Specifically, DHS and DOJ personnel would be permitted to take action against drones for the “safety, security or protection” of a “covered facility or asset.” “Covered facility or asset,” according to the bill, refers to operations near the U.S. Coast Guard and U.S. Customs and Border Protection; DOJ operations; Federal Bureau of Prisons; National Special Security Events; federal law enforcement investigations; and other mass gatherings. Additionally, the bill allows the DOJ and DHS to “detect, identify, monitor and track [drones] without prior consent, including by means of intercept or other access of a wire communication, an oral communication or an electronic communication used to control the [drone].” Further, the bill would allow the DOJ and DHS to “disrupt control” of the drone, and “seize or exercise control” of the drone, as well as confiscate or “use reasonable force to disable, damage or destroy” the drone. The supporters of the bill say that threats posed by malicious drones are too great to ignore. Senator John Hoeven (R – ND) said, “Developing UAS detection and counter-UAS technologies is a key component necessary for us to safely integrate [drones] into our national airspace. This legislation provides the [DHS] and [DOJ] with the tools they need to protect against [drone] threats to our national security, which will help to ensure the safe use of legitimate [drones] so this industry can continue to grow and develop.” *Read more*

Revised Restrictions on Drone Operations Over DoD Facilities

The Federal Aviation Administration (FAA) has previously used its authority under Title 14 of the Code of Federal Regulations sec. 99.7 (“Special Security Instructions”) to address the potential threat posed by malicious drone operations by creating unmanned aircraft system (UAS or drone) specific airspace restrictions over select, national security-sensitive locations at the request of the U.S. Department of

Defense (DoD). This week, the FAA has modified those restrictions. *Read more*

PRIVACY TIP #140

Your Cellphone Location Is Being Sold and Leaked

This week's privacy tip addresses data aggregators and how the four largest cellular providers sell customer data to these third parties. The tip also focuses on the security concerns and permissions issues associated with this practice. *Read more*

© 2018 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.