SpencerFane®

Blogs / Privacy and Cybersecurity Solutions

Toggle Navigation

BLOG EDITORS

Stacy Harper
T 913.327.5120
sharper@spencerfane.com

Shawn Tuma
T 972.324.0317
stuma@spencerfane.com

DATA PRIVACY AND CYBERSECURITY GROUP

- Overview
- Attorneys

Latest Posts

01.22.2019 **EDPB Guidance on GDPR's Jurisdictional Scope**
By Ben Shantz, Thomas W. Hayde, CIPP/US

For many U.S. organizations, figuring out whether – and to what extent – Europe's General Data Protection Regulation ("GDPR") applies to your operations has caused a lot of headaches. Do you have an "establishment in the [European] Union"? Are you "offering…goods and services…to…data subjects in the Union"? Are you "monitoring" the behavior of data subjects in the Union? How will these terms be interpreted and enforced?

01.14.2019 **New South Carolina Insurance Data Security Act**
By Jeremy Rucker

South Carolina has recently enacted a new insurance data security law entitled the South Carolina Insurance Data Security Act. The new legislation generally applies to licensees (any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered, under the insurance laws of South Carolina) with ten or more employees or independent contractors.

01.07.2019 **Cyber Resolutions for the New Year**
By Stacy Harper

As we enter 2019, social media is flooded with resolutions for self-improvement, let us propose a few:

11.06.2018 **Notice – Colorado Changes to Data Privacy Laws**
By Paul J. Hanley

Three major changes to Colorado data privacy laws became effective September 1, 2018. These affect virtually all business collecting personally identifying information (PII)[1] from Colorado residents:

10.24.2018 **Updated Tools for Your HIPAA Toolkit: Medical Record Fees**
By Donn Herring

A Missouri federal court granted a motion to dismiss this week in a case against a provider and medical record processing company. In the case, a patient alleged that a "search and retrieval" fee imposed in response to a patients request for access to medical records violated the Missouri Merchandizing Practices Act. In dismissing the claim, the court only addressed Missouri law as the allegations did not involve alleged violations of HIPAA. The outcome in this Missouri case is similar to the outcome in an unrelated Tennessee case against the same medical records company that was dismissed earlier this summer. The Tennessee case alleged multiple violations of Tennessee law relating to the fees imposed for access to medical records, using HIPAA as the standard for medical records fees. In dismissing the case, the Tennessee court found that neither HIPAA nor Tennessee law provide a private cause of action for excessive medical record fees. The Tennessee case is pending appeal.

10.17.2018 **Updated Tools for Your HIPAA Toolkit: Security Risk Assessment**
By Stacy Harper

In the wake of the record setting $16 Million dollar settlement and resolution agreement with Anthem, Inc, the Office for Civil Rights (OCR) and Office of the National Coordinator for Health Information Technology (ONC) released a new version of their Security Risk Assessment tool. The new tool and recent settlement agreement renew the emphasis of OCR on the performance of HIPAA Security Risk Assessments by covered entities and their business associates.

05.02.2017 **Shopping for Cyber Insurance? Initial Lessons Learned from the Courts**

By Patrick J. Whalen

The burgeoning multi-billion dollar cyber insurance market is expected to continue its 25%+ annual growth over the next few years. Despite this dramatic growth, the market is plagued with uncertainty over the meaning of key policy terms and scope of coverage. The lack of both uniformity in cyber policy language and judicial guidance interpreting policy language prevent companies from confidently assessing their loss exposure in the event of a major data breach.

03.08.2016 **Yet Another Data Sheriff In Town: CFPB Issues Its First Data Security Enforcement Action**

By Thomas W. Hayde, CIPP/US

On March 2, 2016, the CFPB finalized a Consent Order with Dwolla, an online payment platform, for violations of the CFPA. It is the CFPB's first enforcement action related to data privacy and security. It is notable because Dwolla appears to have become an enforcement target due solely to its robust claims about security, and not due to any data breach. It also places obligations on Dwolla's Board to become responsible for data privacy and security in the company.

03.03.2016 **EU-US "Privacy Shield" Disclosed to the Public**

By Thomas W. Hayde, CIPP/US

The past week has seen two key developments in EU-US data privacy relations — the US enacted the Judicial Redress Act into law, and EU and US officials published the proposed EU-US Privacy Shield protocol for transatlantic data transfers. While the Privacy Shield still has a gauntlet of EU bureaucracy to navigate, companies that relied on Safe Harbor should begin to plan now to comply with the robust new requirements of Privacy Shield, or implement other measures to satisfy the EU Privacy Directive to import EU data to the US.

02.11.2016 **President Obama Goes Big on Privacy and Cybersecurity**

By Thomas W. Hayde, CIPP/US

As part of a massive new initiative, Obama establishes the Federal Privacy Council and a national commission on cybersecurity

1 2 3 › Showing 1-10 of 21 results View All