![Mintz logo](M MINTZ)

What We're Reading – September 17, 2021

September 17, 2021 | Blog | By **Cynthia J. Larose**

Ransomware Roundup

It is difficult to keep up with the constant news on ransomware, but here is some of the latest:

Sanctions for Payment? The Wall Street Journal reports that sanctions for payment of ransomware via cryptocurrency may be coming, courtesy of the Department of the Treasury. Read about proposal **here** (subscription may be required).

Russia and Ransomware: The **FBI says** that nothing has changed, despite President Biden's discussion of Russia's harboring of ransomware gangs with Russian President Vladimir Putin.   As a matter of fact, the REvil ransomware group has apparently returned from its "summer break."

Microsoft Finds Link to Ransomware Operations: If your organization has not yet applied the latest Microsoft security patches, you'd best get moving. Microsoft has linked a recently patched vulnerability which was exploited via malicious Office documents to known ransomware operators. **Read more here**.

Ad Tech and Privacy

Big changes are on the move for digital advertising via Apple and Google, potentially increasing the cost of customer acquisition for brands. Since Apple began asking users whether they would allow their online activity to be tracked, only a small percentage have agreed. **Read more.**

And, how will the ecommerce ecosystem market without third party cookies?   It will be a challenge, but first party data – data companies have already acquired, or acquire from consumers with consent – will be the gold standard. **Read more**.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.