White and Williams LLP

Don't You (Forget About Me 2020): Cybersecurity Developments for 2020 in Five Musical References

Cyber Law and Data Protection Alert | **January 12, 2021**

By: Joshua A. Mooney

Is it hyperbolic to say that never before have we seen a quieter, yet more anticipated and welcome end to a year than in 2020? For some, 2020 is a year the sooner forgotten, the better. In data privacy and security law, a lot happened. Here are five musical references to remind what a tremendous year 2020 was.

1. **California Dreamin'**. In January 2020, the California Consumer Privacy Act (CCPA) become effective. Yes – that's hard to believe, given that it feels like we've been talking about CCPA forever. Certainly CCPA lived up to the hype. The three sets of draft regulations released by the California Office of the Attorney General helped, as did the class action litigation. And now, we have the California Privacy Rights Act (CPRA) to close out 2020.
2. **3.15.20**. March 2020 may be remembered best as the month in which cities and states began to shelter-in-place. In data privacy and security, March 2020 saw three big events. First, the U.S. workforce transitioned from onsite operations to remote operations in a millisecond. For many organizations, this shift created vulnerabilities and expanded risk vectors in data security caused by inadequate remote access systems, expanded "bring your own device" policies, or both. There are some steps organizations may take to reduce threats related to remote operations. The full consequence of this workforce shift has yet to be realized. Second, data security requirements under the New York SHIELD Act, including the mandate that organizations have a comprehensive data security program, went into effect. Third, the Illinois appellate court in *West Bend Insurance v. Krishna* held that an oft-cited exclusion in CGL policies did not apply to claims brought under the Illinois Biometrics Information Privacy Act (BIPA). The case breathed additional life into this emerging, cottage-industry litigation.
3. **Suddenly, Last Summer**. In May, the *In re Capital One* decision held that a computer forensics report prepared by a third-party forensics firm through outside breach counsel after a cyberattack was not privileged and subject to discovery in the ensuing class action litigation. The opinion was affirmed by the federal court for the Eastern District of Virginia in June. The decision has required in-house and outside counsel alike to rethink on how to retain and employ forensics firms in the wake of a successful cyberattack. In July, the Court of Justice of the EU (CJEU) decided *Schrems II*, which (a) struck down the Privacy Shield, and (b) has thrown into question whether Standard Contractual Clauses (SCCs) may effect a lawful transfer of data from the European Economic Area (EEA) to the U.S. (*Hint* – many EU regulators say that they do not.) Third, on August 14, 2020, the "final" draft of CCPA regulations were released by the California Office of the Attorney General and went into immediate effect. This would be it – there would be no more changes, right?
4. **October**. On October 1, the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) issued advisories warning ransomware victims, their insurers, and their incident response teams of potential sanctions for facilitating ransomware payments to a person or organization on OFAC's Designated Nationals and

Blocked Persons List (SDN List). The advisories have garnered a fair amount of criticism. They certainly have created a need for companies and cyber insurers to revisit response procedures for ransomware attacks. Oh, also in October, the Information Commissioner's Office (ICO) finally issued fines against Marriot and British Airways, both at significantly lower amounts than the ICO's initial June 2019 notices of intent. Two takeaways for this development: the data breaches involved errors, not intentional data misuse, and both companies are in industries economically ravished by the pandemic.

5. **Late November**. In follow up to the CJEU's ruling in *Schrems II*, the European Data Protection Board (EDPB) adopted for public comment draft recommendations for supplementary measures for transferring personal data outside the EEA. The document, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," is intended to help companies comply with the EU-level of required protections of personal data when such data is transmitted outside the EEA under the SCCs. Separately, the European Commission also published a draft set of revised SCCs for public comment into December, and the CPRA was passed.

If you have questions or would like further information, please contact Joshua A. Mooney (mooneyj@whiteandwilliams.com; 215.864.6345).