Articles + Publications | January 2021

More Privacy, Please – January 2021

WRITTEN BY

David N. Anthony | Ronald I. Raether Jr. | Ashley L. Taylor, Jr. | Angelo A. Stio III | Wynter L. Deagle | Brett A. Dorman | Sharon R. Klein

Do you want a simple way to keep current on important privacy changes? Avoid sleepless nights wondering whether you missed a privacy speed bump or pothole between annual updates? Worry no longer. Troutman Pepper is pleased to offer *More Privacy, Please* — a monthly newsletter recapping significant industry and legal developments, as well as trends in the areas of cybersecurity, information governance, and privacy.

U.S. LAWS AND REGULATION

- **The California AG Releases Fourth Set of Proposed Modified CCPA Regulations.** On December 10, 2020, the California attorney general released a fourth set of proposed modifications to the implementing regulations of the California Consumer Privacy Act (CCPA). If adopted, the proposed modifications would (1) require businesses that sell personal information collected offline to inform consumers (by an offline method) of their right to opt out and how to submit an opt-out request, and (2) revive the option for a business to use an opt-out button for online opt outs, in addition to posting a notice of right to opt out and the "Do Not Sell My Personal Information" link. As the CCPA and its implementing regulations continue to change — most recently with the passage of the California Privacy Rights Act of 2020 — businesses should continue to monitor developments relating to the CCPA, including any additional modifications to the regulations and guidance from the California attorney general. For more information about the latest proposed CCPA regulations, please see Troutman Pepper article, "California AG Releases Fourth Set of Proposed Modifications to CCPA Regulations."

- **New CCPA Requirements Under AB-713 Take Effect January 1, 2021.** In September 2020, AB-713 amended the CCPA to better align with de-identification standards under the federal Health Insurance Portability Act of 1996 (HIPAA). Importantly, beginning January 1, 2021, AB-713 requires any contract for the sale or license of de-identified information, where one of the parties is a person residing or doing business in California, to include (1) a statement that the de-identified information being sold or licensed includes de-identified patient information, (2) a statement that re-identification, and attempted re-identification, of the de-identified information by the purchaser or licensee of the information is prohibited, and (3) a requirement that, unless otherwise required by law, the purchaser or licensee of the de-identified information may not further disclose the de-identified information to any third party unless the third party is contractually bound by the same or stricter restrictions and conditions. For more information related to AB-713, please see Troutman Pepper articles, "CCPA Amendment Further Harmonizes with HIPAA and Provides Additional Exemptions" and "AB-713 CCPA Requirements Take Effect January 1, 2021 for Use of De-identified Health Data Sets."

- **HHS Proposes Modifications to the HIPAA Privacy Rule.** On December 10, 2020, the U.S. Department of Health and Human Services (HHS) announced proposed changes to the HIPAA Privacy Rule to support

individuals' engagement in their care, remove barriers to coordinated care, and reduce regulatory burdens on the health care industry. Key modifications contained in the Notice of Proposed Rulemaking include shortening covered entities' time to provide individuals with access to their PHI to no later than 15 calendar days following the request, reducing the identity burden on individuals exercising their right to access, building out capabilities of EHR systems, creating exceptions to the "minimum necessary" standard for individual level of care coordination and case management uses and disclosures, and eliminating the requirement to obtain an individual's written acknowledgement of receipt of a direct treatment provider's Notice of Privacy Practices. Public comments on the proposed modifications are due 60 days after publication of the on the Notice of Proposed Rule Making in the *Federal Register*.

- **Internet of Things Cybersecurity Act of 2020 Signed into Law.** On December 4, 2020, President Trump signed the bipartisan Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (Act) into law. The Act empowers the National Institute of Standards and Technology (NIST) to create cybersecurity standards for internet-connected devices purchased and used by federal agencies. In particular, the Act provides that the cybersecurity standards must include minimum security requirements for managing cybersecurity risks for IoT devices and should take into account secure development, identity management, patching, and configuration management. The standards ultimately developed by NIST under this law will be of particular interest to manufacturers of IoT devices. Government contractors providing IoT devices will be judged on compliance, with such standards effective two years after enactment.

U.S. LITIGATION AND ENFORCEMENT

- **SolarWinds Security Breach.** The recently revealed cyberattacks against numerous U.S. government departments and thousands of public and private sector entities, via compromised SolarWinds software, justifiably rocked the IT and security world. Dating back to March 2020 and allegedly perpetrated by Russia, the attacks compromised the software "signature" of SolarWinds's Orion network monitoring software — the process that uses encryption to assure the integrity of a software update — and distributed malware as a software update. The malware then stealthily exfiltrated valuable intellectual property, confidential and proprietary data, emails, and other important information from victims' systems. The compromise was unknown until prominent cybersecurity firm FireEye, also a victim of the attacks, discovered the malware and reported on the attacks on December 13, 2020. In a December 14 SEC filing, SolarWinds said it believed approximately18,000 entities may have downloaded the Orion update during the March-June 2020 timeframe, which likely included the malware. Multiple plaintiffs' class action and investors' rights firms have already announced investigations into SolarWinds, and at this point, litigation seems like a foregone conclusion. The SolarWinds breach highlights the importance of IT and security vendor risk management. Organizations should consider requiring third-party vendor contracts to include provisions mandating notification of a vendor's data security incident, providing for indemnification for claims and costs arising out of a vendor's data breach, and excluding data security incidents from liability caps.

- **Dish Network $210 Million Settlement for Telemarketing Violations.** Dish Network recently agreed to pay $210 million to resolve a decade-long lawsuit brought by the U.S. government and four states concerning allegations that millions of unlawful telemarketing robocalls were made on Dish's behalf to consumers on the Do Not Call registry. The settlement comes after Dish's appeal to the Seventh Circuit Court of Appeals, which upheld the lower court's judgement and injunction, but vacated damages and penalties awarded. According to the December 4, 2020 Stipulated Order for Monetary Judgment, the U.S. will receive $126 million, and California, Illinois, North Carolina, and Ohio will split the remaining $84 million. Further, the settlement required Dish to hire a telemarketing compliance expert and demonstrate compliance with various telemarketing rules.

- **SkyMed International Enters into Consent Agreement with FTC.** On December 16, 2020, SkyMed International, Inc. entered into a consent agreement with the Federal Trade Commission (FTC) to resolve allegations that SkyMed engaged in unfair and deceptive acts or practices in violation of Section 5 of the FTC Act by (1) placing a HIPAA seal on every page of its website, which the FTC asserted falsely "signaled to consumers that a government agency or other third party had reviewed SkyMed's information practices and

determined that they met HIPAA's requirements"; (2) failing to provide reasonable security for collected personal information; and (3) providing false information to consumers regarding whether a publicly accessible database included health information and whether a third party improperly accessed that data. Under the proposed settlement agreement, SkyMed must perform a risk assessment, implement and maintain safeguards to protect personal information, obtain biennial assessments of its security program by an FTC-approved third party, and provide annual certification by a senior executive on SkyMed's compliance with the settlement requirements.

INTERNATIONAL REGULATION AND ENFORCEMENT

- **EU-UK Trade Deal Keeps Personal Data Flows Open Without the Need for Additional Safeguards.** On December 24, 2020, the European Union (EU) and the United Kingdom (U.K.) reached an agreement in principle on the long-awaited and historic EU-UK Trade and Cooperation Agreement (Agreement). Once formally adopted, the Agreement will govern the relationship between the EU and U.K. beginning on January 1, 2021 — the end of the Brexit transition period. While the Agreement does not include a determination that the U.K. provides an adequate level of protection for personal data, it includes a further transition period of up to six months to enable the European Commission to complete an adequacy assessment of the U.K.'s data protection laws. In the meantime, personal data may continue to move freely between the EU and U.K. since those transfers are not considered transfers of personal data to a third country, and thus not prohibited by the General Data Protection Regulation (GDPR).

- **IAB Europe Releases a DPIA Guide for Digital Advertising Under GDPR.** IAB Europe — an organization providing analysis and guidance on EU privacy and data protection rules as they apply to the digital advertising sector — released "The GDPR Data Protection Impact Assessments (DPIA) for Digital Advertising under GDPR" (Guide). While there is no one-size-fits-all method, the Guide breaks down who within the organization (or required third parties) should be involved in the process, how to establish/identify the objectives and context of processing, privacy by design and minimization techniques, how to evaluate and assess risks, and mitigation considerations. Additionally, the Guide provides a non-exhaustive list of common risks from processing activities to help organizations identify potential harmful impacts that may occur from processing a data subjects' personal information.

- **Brazilian Data Protection Authority Issues First Guidance on General Personal Data Protection Law.** On December 8, 2020, the Brazilian Data Protection Authority released a Frequently Asked Questions (FAQ) guide, available only in Portuguese, which offers guidance on the General Personal Data Protection Law (LGPD). The FAQ provides guidance on the LGPD's applicability, the legal basis for processing personal data, the rights of data subjects, and actions that public and private organizations must take in order to comply with the LGPD.

UPCOMING WEBINARS

- **Five Key Developments in the Privacy and Data Security Sector in 2020 and Five Predictions for 2021 – Tuesday, January 26, 2021 at 3:00 p.m. ET / 12:00 p.m. PT.** With 2020 now safely behind us, please join our panel of privacy experts and thought leaders for a discussion on the five most important changes in the privacy and data security landscape in 2020 and their opinions on likely developments in 2021.

- **Annual eDiscovery Updates – Wednesday, January 27, 2021 at 12:00 p.m. ET / 3:00 p.m. PT.** Please join members of the eMerge team as they analyze the key decisions, developments, and technical innovations impacting discovery in 2020 and highlight trends for 2021. We will discuss the practical considerations of balancing legal requirements with rapidly evolving technology, including the increased use of collaboration platforms and messaging applications, machine learning and AI, and structured data analytics.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber