AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2022
VOL. 8 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 2** **February-March 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [2] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Privacy & Cybersecurity Developments

*By Sharon R. Klein, Alex C. Nisenbaum, Karen H. Shin and David J. Oberly**

STATE AND LOCAL LAWS AND REGULATION

Virginia Consumer Data Protection Act Work Group Issues Final Report

The Virginia Consumer Data Protection Act Work Group ("Work Group") released its final report.[1] The Virginia Consumer Data Protection Act ("VCDPA") requires the chair of the Virginia Joint Commission on Technology and Science to set up the Work Group to review the provisions of the VCDPA and discuss issues relating to its implementation. Points of emphasis and recommendations cited by the Work Group in its final report include submitting a budget amendment to fund a small staff to lead VCDPA enforcement on day one of enactment, allowing the state attorney general to pursue actual damages based on consumer harm, authorizing consumers to submit opt-out requests via a global opt-out setting, sunsetting the "right to cure" provisions, amending the right to delete under the VCDPA to be a right to opt out of sale to restrict further dissemination of personal data, and directing a Virginia state agency to promulgate VCDPA-related regulations. The Work Group's recommendations will be presented to the Virginia legislature in its upcoming session and could influence potential amendments to the VCDPA ahead of its January 1, 2023, effective date.

New York Requires Notification to Employees for Electronic Monitoring

New York Governor Kathy Hochul signed S2628[2] into law, requiring employers with a place of business in New York who engage in electronic monitoring of telephone, e-mail, and internet access or usage to provide written notice upon hiring to employees subject to such electronic monitoring. The written notice must be conspicuously posted and readily available for viewing by employees and must be acknowledged by employees in writing or electronically. The New York Attorney General has enforcement authority and violations of S2628 result in a maximum civil penalty of $500 for the first offense,

* Sharon R. Klein (sharon.klein@blankrome.com), a partner at Blank Rome LLP and chair of the firm's Privacy, Security & Data Protection practice, advises businesses on risks related to the privacy and security of personal data, artificial intelligence data, implementing privacy, security, and data protection policies and best practices, and compliance with global, federal, and state privacy and security laws. Alex C. Nisenbaum (alex.nisenbaum@blankrome.com), a partner at the firm, advises clients on data privacy and information security laws and regulations, including compliance with HIPAA/HITECH; Gramm-Leach-Bliley; the California Consumer Privacy Act; cross-border data transfer; and state privacy, data protection, and breach notification requirements. Karen H. Shin (karen.shin@blankrome.com) is an associate at the firm focusing her practice on a variety of data privacy and information security matters. David J. Oberly (david.oberly@blankrome.com), an associate at the firm, counsels and represents clients in a range of biometric privacy, data privacy, and data security/cybersecurity compliance, risk management, and class action litigation matters.

[1] https://rga.lis.virginia.gov/Published/2021/RD595/PDF.

[2] https://www.nysenate.gov/legislation/bills/2021/s2628.

$1,000 for the second offense, and $3,000 for the third and each subsequent offense. S2628 does not apply to processes that are: (1) designed to manage the type or volume of incoming or outgoing e-mail or telephone voice mail or internet usage; (2) not targeted to monitor or intercept the e-mail or telephone voice mail or internet usage of a particular individual; and (3) are performed solely for the purpose of computer system maintenance and/or protection.

FEDERAL LAWS AND REGULATION

Introduction of Protecting Sensitive Personal Data Act

United States Senators Marco Rubio (R-FL) and Raphael Warnock (D-GA) introduced the Protecting Sensitive Personal Data Act,[3] which expands the U.S. Department of the Treasury's Committee on Foreign Investment's ("CFIUS") oversight authority of transactions involving sensitive personal data. Currently, there are limited circumstances in which CFIUS is able to require companies to make a mandatory declaration prior to completing a transaction. The bill would expand the CFIUS' authority to issue regulations that require mandatory declarations to foreign investments in U.S. companies that handle sensitive personal data, which includes genetic test results, health conditions, insurance applications, financial hardship data, security clearance information, geolocation data, private e-mails, data for generating government identification and credit report information.

CISA Releases Operational Directive Order Requiring Federal Agencies to Remediate Cyber Vulnerabilities

The Department of Homeland Security's Cybersecurity Infrastructure and Security Agency ("CISA") issued Binding Operational Directive 22-01[4] (the "Directive") requiring federal agencies to remediate vulnerabilities in accordance with the CISA-managed vulnerability catalog[5] (the "Catalog"). The Catalog will list exploited vulnerabilities that carry significant risk to the federal enterprise and require federal agencies to remediate vulnerabilities with a Common Vulnerabilities and Exposures ("CVE") ID assigned prior to 2021 within six months and all other vulnerabilities within two weeks. The Directive also required federal agencies to, by January 2, 2022, review and update agency internal vulnerability management procedures, including providing a copy of those procedures to CISA upon request. Additionally, federal agencies must report on the status of listed vulnerabilities through the Continuous Diagnostics and Mitigation ("CDM") Federal Dashboard.

---

[3] https://www.rubio.senate.gov/public/_cache/files/b59c64e5-3398-462e-95f4-82322247134d/AAD230C43594EAC27C4956BD4CB58C64.protecting-sensitive-personal-data-act---bur21312.pdf.

[4] https://cyber.dhs.gov/bod/22-01/.

[5] https://www.cisa.gov/known-exploited-vulnerabilities.

Department of Defense Announces Cybersecurity Maturity Model Certification 2.0

The U.S. Department of Defense ("DoD") announced[6] the strategic direction of the Cybersecurity Maturity Model Certification ("CMMC") program. The DoD stated that the "CMMC 2.0," which will not be effective until the DoD issues rules for the program, will maintain the program's goal of safeguarding sensitive information while simplifying CMMC standards and providing clarity on requirements, focusing advanced cybersecurity standards and third party assessment requirements on companies supporting the highest priority programs, and increase DoD oversight of professional and ethical standards for assessments.

CMMC 2.0 seeks to reduce compliance burden on contractors that may not hold particularly sensitive data or support high-priority programs by allowing them to conduct self-assessments and attest to their compliance with CMMC standards. While this may reduce certification burdens for contractors that are able to take advantage of self-attestation, it may not necessarily reduce compliance risk for such contractors in light of the U.S. Department of Justices' recently announced Civil Cyber Fraud Initiative,[7] emphasizing enforcement against contractors that "put U.S. information or systems at risk." Accordingly, companies that may self-attest when CMMC 2.0 rules become effective should invest in appropriate processes designed to promote accurate internal cybersecurity assessments and reporting.

Federal Banking Regulator Final Rule on Bank Incident Reporting:

The U.S. Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation ("FDIC") approved a final rule[8] to improve the sharing of information about cyber incidents that may affect the U.S. banking system (the "Final Rule"). The Final Rule requires banks to notify their primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after they determine that a cyber incident has occurred.

Notification is required for incidents that have materially affected or are reasonably likely to materially affect the viability of a bank's operations, its ability to deliver banking products and services, or the stability of the financial sector. The Final Rule also requires a bank service provider to notify affected bank customers as soon as possible after determining it has experienced a computer-security incident that has materially affected or is reasonably likely to materially affect customers for four or more hours. Compliance with the Final Rule is required by May 1, 2022.

---

[6] https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/.

[7] https://www.blankrome.com/publications/department-justice-prioritize-cybersecurity-fraud-through-new-civil-cyber-fraud.

[8] https://www.occ.treas.gov/news-issuances/news-releases/2021/2021-119a.pdf.

Reintroduction of Online Privacy Act

United States Representatives Anna Eshoo (D-CA) and Zoe Lofgren (D-CA) reintroduced the Online Privacy Act,[9] which was previously introduced in 2019. The revised bill continues to provide individuals the rights to access, correct, and delete their personal information as well as the right to request human review of automated decisions. The revised bill additionally provides individuals the right to decide how long companies can retain their data. The revised bill also continues to provide for the creation of the Data Privacy Agency ("DPA") to enforce the Online Privacy Act.

However, the revised bill establishes an Office of Civil Rights within the DPA and authorizes state privacy regulators, such as the California Privacy Protection Agency, to enforce the Online Privacy Act alongside state attorneys general. The Online Privacy Act also sets forth obligations for companies, including but not limited to requiring companies to articulate the need for and minimize the data they collect, process, disclose, and maintain; not disclose or sell personal information without explicit consent; not use dark patterns to obtain consent; employ reasonable cybersecurity policies to protect data; and notify the DPA and affected individuals of breaches and data sharing abuses.

U.S. LITIGATION

Snapchat Investor Class Action Alleges Snapchat Misled on Effect of Apple Privacy Features

Investors filed a putative class action[10] lawsuit against Snap Inc. ("Snap") and company executives, alleging Snap "continuously downplayed and misled investors regarding the impact of Apple's new data privacy features would have on its business." Apple announced the features, which include providing users with the ability to opt out of certain data tracking in June 2020 and released the features in April 2021. The suit alleges that Snap relies on user data for its advertising business and that, following the announcement of the new features, Snap made several statements in SEC filings and quarterly earnings calls that misrepresented or failed to disclose the risks and impact of the changes on Snap's advertising business. According to the suit, it was not until Snap's third quarter 2021 10-Q filing that Snap disclosed the negative effect of the changes to investors. The lead plaintiff claims that investors were damaged by a 26 percent decrease in Snap's share price following the disclosure.

Robinhood Faces Class Action over Data Breach

A class action was filed against Robinhood Markets Inc. ("Robinhood") arising out of a data breach affecting millions of Robinhood users. The complaint alleges that the

[9] https://eshoo.house.gov/sites/eshoo.house.gov/files/OnlinePrivacyActof2021.pdf.

[10] https://fingfx.thomsonreuters.com/gfx/legaldocs/zgvomkaodvd/SECURITIES SNAP PRIVACY complaint.pdf.

breach, which resulted from an attacker socially engineering a Robinhood customer support employee by telephone according to Robinhood regulatory filings, could have been avoided through basic security measures, authentications, and training. The suit asserts negligence, breach of contract, and misrepresentation claims, as well as claims of breach of fiduciary duty and violation of New York's general business law.

SolarWinds Shareholders File Derivative Suit against Company and Directors over Sunburst Attack

A shareholder derivative suit was filed against current and former directors of SolarWinds Inc. ("SolarWinds") claiming directors breached their fiduciary duties by failing to monitor or oversee "any aspect of the company's known mission critical cybersecurity risks." Specifically, the complaint alleges that directors ignored Securities and Exchange Commission and New York Stock Exchange guidelines on cybersecurity oversight and that serious cybersecurity deficiencies persisted at SolarWinds for years, including directing clients to disable firewall and other security protections on SolarWinds software, overseeing cybersecurity budget cuts, and publicly listing sensitive and high-value clients on its website. The derivative suit follows a class action filed against the company on behalf of shareholders in January 2021.

U.S. ENFORCEMENT

Colorado Attorney General Settles Enforcement Action against Construction Company Relating to Data Breach

The Colorado Attorney General's office announced[11] that it settled an action against SEMA Construction ("SEMA") alleging violation of Colorado law requiring companies to take reasonable steps to protect personal sensitive personal information, dispose of such information when it is no longer needed, and promptly notify Colorado residents in the event of a data breach. SEMA was the target of a phishing attack in 2018 that impacted employee e-mail accounts and the personal information of nearly 2000 individuals stored in those accounts.

The Colorado Attorney General alleged that SEMA did not have a data disposal policy in place at the time of the attack and failed to notify some individuals of the breach until nearly two years after it was discovered by SEMA. Under the settlement, SEMA will pay a $63,000 civil penalty and is required to update its security practices to maintain an incident response plan, an information security plan, and an information disposal policy, as well as regularly submit reports regarding its cybersecurity practices to the Colorado Department of Law.

[11] https://coag.gov/press-releases/11-8-21/.

INTERNATIONAL LAWS AND REGULATION

European Parliament Adopts Draft Cybersecurity Directive

The European Parliament Committee on Industry, Research and Energy adopted a draft cybersecurity directive[12] ("NIS 2 Directive"). The NIS 2 Directive is anticipated to replace the existing EU Directive on the Security of Network Information Systems enacted in 2017. The original directive was implemented in different ways by EU member states, fragmenting the EU's approach to cybersecurity. The NIS 2 Directive seeks to harmonize approaches within the bloc. The NIS 2 Directive would also broaden the scope of the existing directive by expanding requirements to "important sectors" such as postal services, waste management, chemicals, food, manufacturing of medical devices, electronics, machinery, motor vehicles, and digital providers in addition to "essential sectors" such as energy, transport, banking and health.

The NIS 2 Directive imposes stronger security requirements using a risk management approach, including mandating requirements for incident response, supply chain security, and encryption and vulnerability disclosure, among other things. It also establishes a framework intended to facilitate better information sharing between governmental authorities and member states to help coordinate management of large-scale cybersecurity incidents. The proposal will now be negotiated by European Parliament legislators to seek agreement on the final form of the NIS 2 Directive.

UK Supreme Court Denies Class Action Lawsuit

The UK Supreme Court issued a decision[13] in *Lloyd v. Google LLC* denying a claim seeking billions of dollars in damages from Google through a class action alleging violations of the UK Data Protection Act of 1998 ("UK DPA"). Lead claimant Lloyd alleged on his own behalf and on behalf of a class of approximately four million iPhone users that Google's use of browser information to track users between August 2011 and February 2012 violated the UK DPA. The UK Supreme Court determined that the DPA did not permit recovery of compensation for mere "loss of control" of personal data, but requires some form of material damage such as financial loss or distress.

The UK Supreme Court further held that a representative claim should not be allowed to proceed because Lloyd was unable to demonstrate that each individual in the class had suffered a violation of their rights and material damages as a result of that violation. Rather, each class member would require an individualized assessment of the impact of the violation, the court stated. The decision will limit such representative claims in the future and provide assurance to companies that technical breaches of UK data protection law that do not result in material damages will not support an award for damages in future claims.

---

[12] https://www.europarl.europa.eu/news/en/press-room/20211022IPR15610/cybersecurity-meps-strengthen-eu-wide-requirements-against-threats.

[13] https://www.supremecourt.uk/cases/docs/uksc-2019-0213-judgment.pdf.

Draft Implementing Regulations for China's Personal Information Protection Law and Data Security Law Released

The Cyberspace Administration of China ("CAC") released a draft of the Administrative Regulations on Network Data Security[14] (the "Regulations") for China's Personal Information Protection Law and Data Security Law. Highlights of the Regulations include:

(1) Requiring organizations to notify affected individuals of data security incidents that cause harm within three working days and report incidents involving the personal data of more than 100,000 people to the provincial-level CAC branch within eight hours and submit a written incident report within five working days;

(2) Establishing a security gateway through which all data transferred out of China must pass;

(3) Requiring organizations to respond to data subject requests within 15 working days;

(4) Requiring organizations transferring personal data outside of China to submit an annual data exit assessment report to the provincial-level CAC by January 31 of each year; and

(5) Requiring a cybersecurity review and approval from the CAC for certain data processors, including those listed outside of Mainland China if they process personal information of more than 1,000,000 people and those listed in Hong Kong if their activities may affect national security.

EDPB Issues Draft Guidelines on International Data Transfers

The European Data Protection Board ("EDPB") adopted guidelines on the interplay between Article 3 and Chapter V of the General Data Protection Regulation ("GDPR")[15] (the "Guidelines") to assist controllers and processors in the European Union in identifying whether a processing operation constitutes an international transfer, and to provide a common understanding of the concept of international transfers.

The Guidelines specify three cumulative criteria that qualify a processing as a transfer: (1) the data exporter (a controller or processor) is subject to the GDPR for the given processing; (2) the data exporter transmits or makes available the personal data to the data importer (another controller, joint controller, or processor); and (3) the data importer is in a third country or is an international organization. The processing will be considered a transfer, regardless of whether the importer established in a third country

[14] https://mp.weixin.qq.com/s/Cv2BS9tF_OQvq9vUxqqQUw.

[15] https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf.

is already subject to the GDPR under Article 3 GDPR. However, the EDPB considers that collection of data directly from data subjects in the EU at their own initiative does not constitute a transfer.