Simpson Thacher

Memorandum

Privacy Law Update: Colorado, California, New York, GDPR and the Supreme Court

July 13, 2021

This memorandum offers important practice tips with respect to several recent privacy law developments.[1]

The Colorado Privacy Act ("CPA")

Scope: On July 7, 2021, Colorado Governor Jared Polis signed the CPA[2], which will take effect on July 1, 2023 and become the third comprehensive state consumer privacy law in the United States. The CPA applies to legal entities that (a) conduct business in Colorado or produce products or services that are intentionally targeted to Colorado residents and (b) that either: (1) control or process personal data of more than 100,000 Colorado residents per year; or (2) derive revenue from the sale of personal data and control or process the personal data of at least 25,000 Colorado residents per year.

Exemptions: The CPA excludes (i) HIPAA-covered information; (ii) financial institutions and affiliates regulated under the Gramm-Leach-Bliley Act; (iii) data covered by the Fair Credit Reporting Act, the Children's Online Privacy Protection Act and a few other statutes; (iv) de-identified data (except for a limited oversight obligation); (v) data of individuals in an employment or business context; or (vi) data from government records or that is reasonably believed to be publicly available. The CPA has exemptions for data processing for certain specified reasons (*e.g.*, internal operations and cooperation with law enforcement).

Overlap with Earlier Laws: If your organization is currently subject to and complies with the GDPR and CCPA, then it already substantially complies with the CPA, because it should already: (i) disclose how and why it processes and discloses personal data; (ii) post consumers' "opt out" rights in certain circumstances; (iii) use reasonable data security practices; (iv) not use personal data unnecessarily or discriminate against consumers for exercising their data rights; (v) conduct required data impact assessments; (vi) include data privacy terms in its relevant vendor contracts; (vii) comply with its obligations in its role as a data controller or processor; and (viii) respond to consumer requests regarding personal data.

[1] This memorandum provides only a high-level summary of these laws and developments. For a more detailed discussion, please consult one of the authors of this memorandum.

[2] S.B. 21-190, 73d Leg., 1st Reg. Sess. (Co. 2021).

Enforcement: There is no private right of action for CPA violations. The Colorado Attorney General or district attorneys may sue (but organizations are given a 60-day cure period before prosecution, only until January 1, 2025).

Practice Tip: The CPA has a few new obligations compared to other privacy laws. *First*, covered companies must post in their privacy policies the right of Colorado residents to opt out of targeted advertising, sales of their data or certain profiling activities, which is broader than the scope of "opt out" activities provided in other state laws. *Second*, companies should conduct a "data protection assessment" for processing that presents a heightened risk of harm to Colorado residents, a concept introduced for state residents in the California and Virginia laws.

The California Privacy Rights Act

The California Privacy Protection Agency ("CPPA") Board, established by the recently enacted California Privacy Rights Act ("CPRA"), held its first board meeting on June 14, 2021. The CPPA will have the power to implement and enforce the CCPA and CPRA on January 1, 2023. The CPRA amends the California Consumer Privacy Act by, inter alia: (i) subjecting "sensitive" personal information to additional use, opt-out and disclosure requirements; (ii) eliminating the 30-day cure period before a business can be fined for non-compliance; (iii) adding required provisions to service provider agreements; (iv) requiring opt-out notice for sharing of data in cross-context behavioral advertising; and (v) requiring annual cybersecurity audits and risk assessments in certain circumstances.

Practice Tip: As the CPPA is the first U.S. or state administrative agency dedicated solely to privacy matters, it is expected to be active in enforcement. CPRA will cover personal data collected after January 1, 2022, so companies should be working now on their compliance program. Regulations to supplement certain CPRA provisions (including access and opt-out rights) are expected in the coming months.

N.Y. Department of Financial Services Issues Ransomware Guidance

On June 30, 2021, the New York State Department of Financial Services ("DFS"), which regulates companies engaged in banking, insurance and financial services in New York, issued guidance on preventing ransomware attacks.[3] The guidance is intended to help companies combat the most common ransomware techniques and urges every company, regardless of size, to implement a cybersecurity program, and every DFS-regulated company to implement as many as possible of the controls outlined by the DFS.

Practice Tip: The DFS recommends:

- anti-phishing training for employees, along with company-wide email filtering systems;

[3] New York Department of Financial Services, RANSOMWARE GUIDANCE, (2021). (https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance)

- creating documented programs to identify, assess, track, and remediate vulnerabilities on all enterprise assets, as well as periodic penetration testing;
- multi-factor authentication for remote access to networks, all externally exposed enterprise and third-party applications, and all logins to privileged accounts;
- disabling remote desktop protocol access from the Internet, whenever feasible;
- using strong, unique passwords with at least 16 characters;
- restricting all service accounts to the minimum access required to complete a job;
- monitoring and responding to alerts of suspicious activity and implementing endpoint detection and response solutions to look for irregular activity;
- maintaining extensive, segregated system backups, with at least one set of system backups isolated from the network and kept offline to prevent hackers from deleting or encrypting them; and
- developing an incident response plan designed to address ransomware attacks.

New Standard Contractual Clauses Under GDPR

On June 4, 2021, the European Commission published its decision approving a new version of Standard Contractual Clauses ("SCCs"), [4] a widely-used EU GDPR-compliant mechanism to transfer personal data from the European Economic Area to countries such as the United States. SCCs have become even more important after July 2020, when the European Court of Justice struck down the EU-U.S. Privacy Shield, a program that had allowed U.S. companies to receive EU personal data if they self-certified as to their privacy law compliance.[5] The new SCCs increase the compliance obligations on data controllers and processors and require the parties to provide significantly more information on the nature of the underlying data processing, conduct a more robust pre-signing evaluation of the risks related to the transfer and to document the entire process in the appended annexes.

Practice Tip: The new SCCs must be used for relevant data transfers made on or after September 27, 2021 and may be used as early as June 27, 2021. Any SCCs entered into prior to September 27, 2021 may continue to be used until December 27, 2022, if the nature of the underlying data processing does not materially change.

[4] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

[5] Until the Privacy Shield is replaced, SCCs or Binding Corporate Rules (which govern intra-company data transfers and require regulators' approval) are the primary mechanism for EU personal data transfers to U.S. companies—the other transfer criteria under the GDPR are of limited scope.

Supreme Court Rules on Anti-Hacking Statute and Privacy Class-Action Suits

The U.S. Supreme Court recently ruled[6] that the federal anti-hacking statute, the Computer Fraud and Abuse Act, 18 USC § 1030(a)(2), is violated by a person's unauthorized *access* to a computer or information stored on it, but not by their *use* of information gained by using valid credentials for an unauthorized purpose. In this case, a police officer had valid credentials to access a law enforcement database, but he sold the information he retrieved, violating department policy. The Supreme Court held that the police officer had not violated the CFAA, because he was legitimately allowed access to the computer system where he took the information he improperly sold.

Practice Tip: To maximize the chances of a successful CFAA claim, be clear in "cease and desist" letters and workplace policies—when it is applicable—that *any* access to your computers, websites and databases (or restricted areas thereof) without consent is prohibited. A clear argument that someone's technical access to your system (or parts of it) was not authorized will likely be needed to support a CFAA claim.

The U.S. Supreme Court also recently ruled[7] that most plaintiffs in a class did not have standing to sue for a violation of the Fair Credit Reporting Act (FCRA) when a credit reporting agency included erroneous information in their credit files, because their files were not actually provided to third parties. The Court held that the plaintiffs did not suffer a sufficiently concrete harm to support standing, because the erroneous information had not gone anywhere. The Court rejected the plaintiffs' argument that the risk of the erroneous information being disseminated in the future was sufficiently concrete to support standing. The Court also denied standing to all of the class members but one on a claim resulting from formatting errors in their files, again due to the absence of any concrete harm. The Court did uphold standing for a smaller set of plaintiffs whose files containing erroneous information were actually sent to third parties.

Practice Tip: The decision was closely watched, due to its implications for class-action lawsuits in response to data security breaches. The appellate and lower courts have issued inconsistent holdings on whether plaintiffs' damages (or potential damages) arising from a data security breach are sufficiently concrete to confer standing to sue, even if a statute has been violated. Companies should continue to act promptly to aid consumers after a data breach, such as by providing credit monitoring services and reimbursing for any fraudulent charges, to have a strong defense on whether a concrete harm has occurred.

[6] *Van Buren v. United States*, 593 U.S. __ (June 3, 2021).

[7] *Transunion v. Ramirez*, 594 U.S. __ (June 25, 2021).

For further information regarding this memorandum, please contact one of the following:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Genevieve Dorment
+1-212-455-3605
genevieve.dorment@stblaw.com

Bobbie Burrows
+1-212-455-2333
bobbie.burrows@stblaw.com

Amy Gopinathan*
+1-212-455-7088
amy.gopinathan@stblaw.com
*Not Yet Admitted

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com

Jonathan S. Kaplan
+1-212-455-3028
jonathan.kaplan@stblaw.com

Jacob Lundqvist
+1-212-455-3348
jacob.lundqvist@stblaw.com

Kate E. Mirino
+1-212-455-2055
kate.mirino@stblaw.com

Alysha J. Sekhon
+1-212-455-3762
alysha.sekhon@stblaw.com

PALO ALTO

Harrison J. (Buzz) Frahn
+1-650-251-5065
hfrahn@stblaw.com

Corina McIntyre
+1-650-251-5073
corina.mcintyre@stblaw.com

Samuel Watters
+1-650-251-5252
samuel.watters@stblaw.com

WASHINGTON, D.C.

Vanessa K. Burrows
+1-202-636-5891
vanessa.burrows@stblaw.com

The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of an attorney-client relationship. Simpson Thacher & Bartlett LLP assumes no liability in connection with the use of this publication. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.