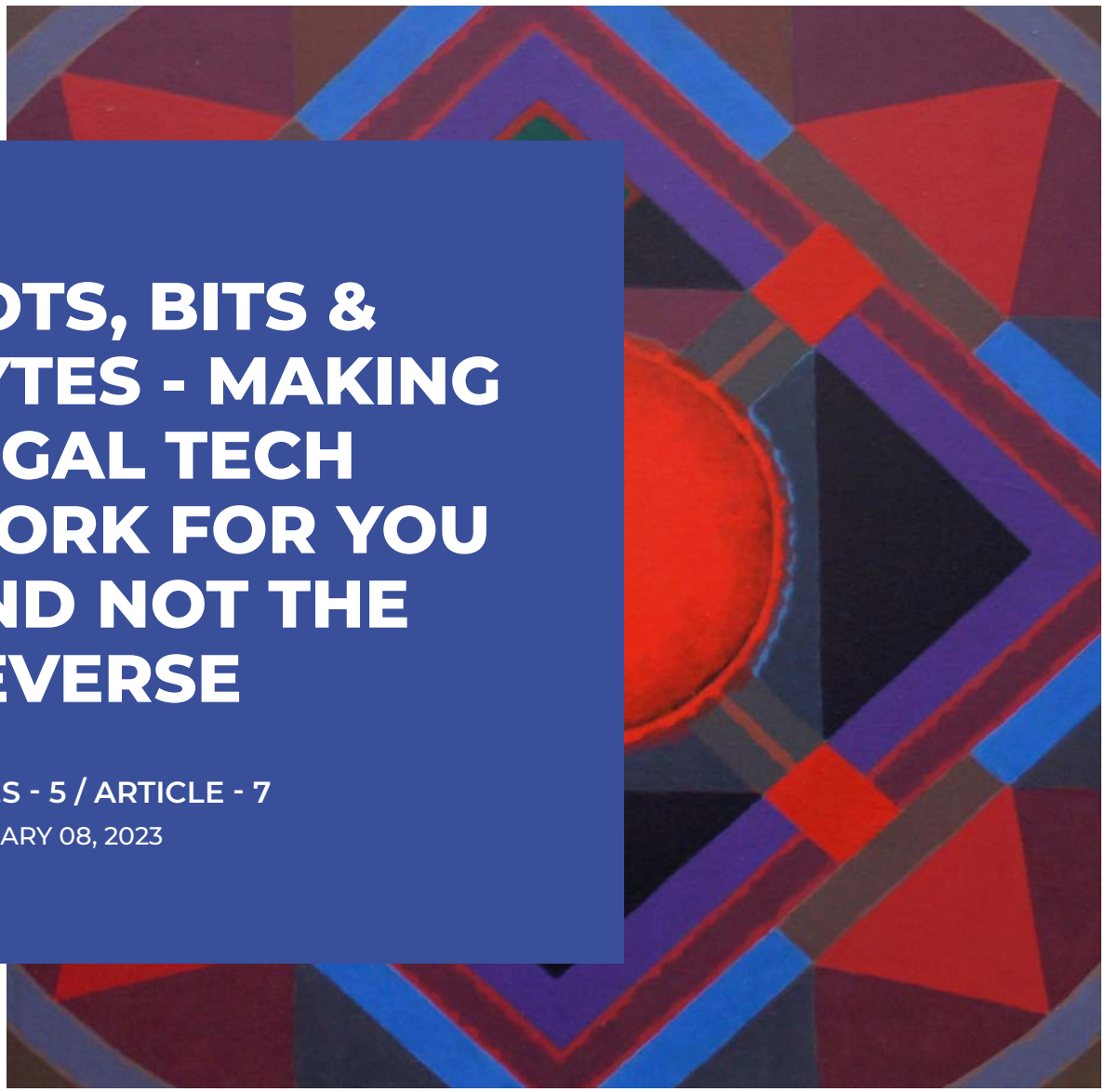
THE NEW DATA PRIVACY RULES FOR 2023



BOTS, BITS & BYTES - MAKING LEGAL TECH WORK FOR YOU AND NOT THE REVERSE

SERIES - 5 / ARTICLE - 7

FEBRUARY 08, 2023

By **Jeffrey Brochin, Esq.**

GreenPoint> Law&Compliance

william.anderson@greenpointglobal.com | pranav.menon@greenpointglobal.com

International Corporate Center, 555 Theodore Fremd Avenue, Suite A102 Rye, NY 10580

www.greenpointlegal.com

In 2018, California passed one of the most sweeping and comprehensive data privacy laws in the country. Known as the California Privacy Protection Act, the statute handed consumers great control over what personal information a business could collect about them. Then in 2020, the state further enhanced that protection by way of the California Privacy Rights Act (CPRA), which went into effect on January 1, 2023. Four other states, Virginia, Colorado, Utah, and Connecticut, have similarly enacted data privacy laws rather than wait for the much-anticipated federal law, which—although it passed in committee by a landslide—has yet to be voted into law. The practitioner would be well-advised to become familiar with these significant changes to consumer data privacy protection.

How the CPRA Protects California Consumers

A primary feature of California's CPRA is the 'right to know' provision, pursuant to which a consumer can request that a business disclose what personal information may have been collected, used, shared, or sold about the consumer. By filing a request, the consumer can find out what specific pieces of information have been collected, the sources from which the business collected the information, and with what category of third-party the data was shared.

The new (2023) provisions, in addition, give the consumer the right to correct inaccurate personal information and to limit the use and further dissemination of sensitive personal information that was collected. Businesses that fall under the CPRA must not only respond to consumer requests but also provide notices explaining what their data privacy practices are. The CPRA also applies to data brokers, which are defined as businesses that knowingly collect and sell a consumer's personal information to third parties—even if the consumer does not have any relationship with such a third party.

What Virginia's CDPA Provides

Virginia became the second state, after California, to pass a comprehensive data privacy law. Known as the Consumer Data Protection Act (CDPA), the law went into effect on January 1, 2023, and was widely hailed by the tech sector as well as by data privacy advocates. Perhaps one reason why the law enjoyed tech industry backing was because of the lack of a private right of action in the CDPA. For starters, the law only applies to businesses that have at least 100,000 customers in Virginia or any business that earns 50 percent of its gross revenue from the sale of personal data and processes personal data for at least 25,000 consumers.

Like California's CPRA, the CDPA also allows consumers to access their private information that has been collected, correct mistakes in that information, and delete data that businesses have collected about them; and the law also has an opt-out feature eliminating data collection altogether. However, unlike the California model, the CDPA does not give consumers the right to sue a business via a private right of action when those rights are violated.

"KEEP AN EYE ON ENFORCEMENT ACTIVITY IN ALL OF THE STATES TO BETTER UNDERSTAND HOW THESE NEW AND COMPLEX REQUIREMENTS ARE INTERPRETED BY THEIR RESPECTIVE ENFORCEMENT AGENCIES."

— Kathleen E. Scott, Partner, Wiley Rein, LLP

Complying with Colorado and Utah Law

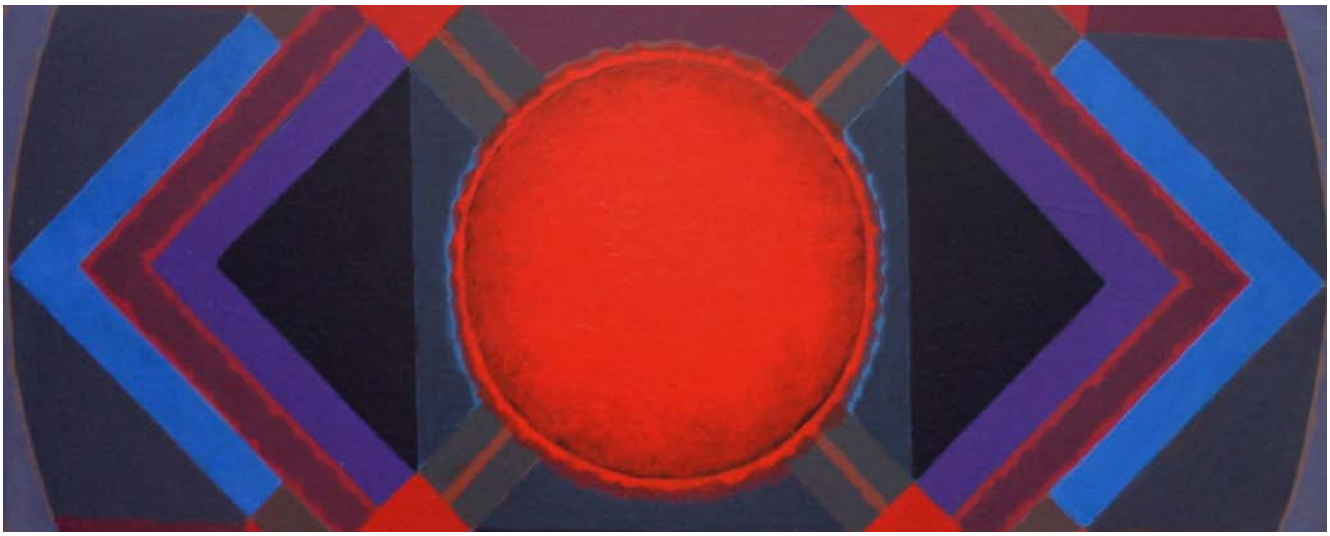
The Colorado Privacy Act (CPA) will go into effect on July 1, 2023, and will apply to business conducted in Colorado that
(1) controls or processes the personal data of 100,000 or more consumers during a year or
(2) controls or processes the personal data of 25,000 or more consumers and derive revenue or receive a discount on the price of goods or services from the sale of personal data; however, the CPA does not state a particular revenue threshold. Furthermore, although the CPA does include as 'consumers' Colorado residents acting in their individual or household contexts, it excludes those individuals acting in a commercial or employment context, job applicants, as well as other categories from its definition of 'consumer.'

To comply with the CPA, businesses will need to provide consumers with clear privacy notices and conduct data protection assessments for any personal data processing that presents a heightened risk of harm to consumers. The CPA does not offer much guidance as to what may or may not qualify as a "heightened risk of harm," but the Colorado Attorney General could promulgate clarifying rules before the CPA goes into effect.

Businesses that operate in or serve Utah residents, including those that control or process personal data, will have to be ready for compliance with the Utah Consumer Privacy Act (UCPA) beginning December 31, 2023. Covered businesses are those with annual revenue of $25M or more that either control or process personal data of 100,000 or more consumers in a calendar year or derive more than 50% of gross revenue from the sale of personal data and control or processes personal data of 25,000 or more consumers.

Connecticut's CTDPA

On May 10, 2022, Connecticut became the fifth state to enact a comprehensive data privacy law, and its effective date will be July 1, 2023. Similar to those data privacy laws enacted by California, Colorado, Virginia, and Utah, the CDPA provides Connecticut consumers with choices as to the personal data collected about them, and it imposes obligations on businesses that handle Connecticut consumer data. Some compliance highlights are that the CTDPA imposes obligations upon 'controllers' and 'processors' of consumer data, with 'controllers' being those who determine the 'purpose and means' of processing personal data, while 'processors' are those who handle data on behalf of a controller. Controllers are specifically required to provide a means for consent and consent revocation when processing sensitive personal data, including race, ethnicity, religion, health conditions, sex life or orientation, citizenship or immigration status, genetic or biometric data, children's data, and precise geolocation data.



The Downside of State Data Privacy Laws

The problem, of course, with five different—and likely growing—state data privacy laws are that this scenario puts an unfair burden on industry, tech sector or not, to keep track of and comply with a host of different laws in different jurisdictions. Given the fact that virtually all commerce, group association, most educational and academic resources, as well as medical, insurance, and financial services, are conducted 'cross-border' vis-à-vis access in every different state, these inconsistencies make it rather easy to land in violation territory. It is for that reason that most industry representatives advocate for a singular, uniform national law not unlike Europe's GDPR.

However, until consensus is reached as to a national code for data privacy protection, industry stakeholders must continue to keep a careful eye on the individual state codes in order to stay in compliance with them. Curiously, some privacy advocacy groups are less keen on a national data privacy law fearing that the national standards—when finally hammered out—might actually prove to be less protective of consumers than California's highly reformist CPRA and those of the other states reviewed above.

Executive Summary

1. The Issue

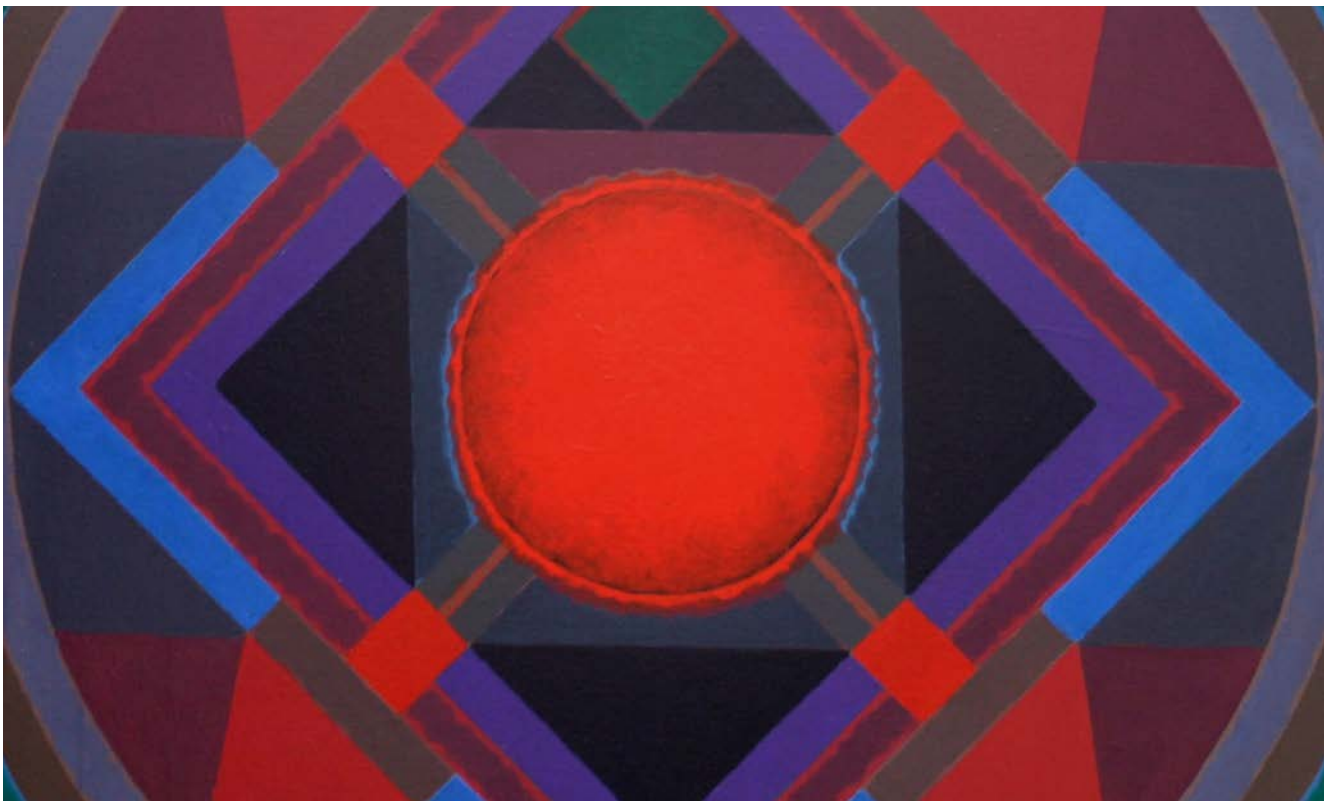
How will the latest state data privacy laws affect practitioners?

2. The Gravamen

Both similarities and differences between the various state enactments must be studied in order to maintain compliance.

3. The Path Forward

In the absence of a uniform national standard for data privacy, keeping abreast of what compliance—and enforcement—of state data privacy laws entail will serve your clients' best interests.



Action Items:

1 California First:

It is recommended that considerable attention be paid to California's CPRA due to the strictness of its statute and the greater likelihood of running afoul of its privacy laws.

2 Status of Your Client:

Pay close attention to whether your client is a 'controller', 'processor', or otherwise falls under any of the state data privacy statutes.

3 Notices to Consumers:

Clients must comply with the specific notices to consumers as to their rights, the option to opt out where applicable, and how requests from consumers will be handled.

4 Which Enforcer:

Different states have different enforcement mechanisms ranging from a private right to sue, Attorney General enforcement, or a new agency created specifically for enforcement; understand what the unique mechanism is in each state that affects your clients.

Further Readings

1. https://www.axios.com/2023/01/03/states-data-privacy-laws-2023
2. https://www.financierworldwide.com/new-data-privacy-laws-in-various-us-states-are-you-ready#.
3. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
4. https://www.reuters.com/legal/legalindustry/us-data-privacy-laws-enter-new-era-2023-2023-01-12/
5. https://www.osano.com/articles/data-privacy-laws
6. https://news.sophos.com/en-us/2023/01/28/data-privacy-laws-compliance-to-take-center-stage-in-2023-and-beyond/

Jeffrey Brochin, Esq.

GREENPOINT STAFF COUNSEL
AND CONTENT EDITOR

After receiving his Juris Doctor degree from The John Marshall Law School in Chicago, Mr. Brochin served as an Administrative Law Judge with the Illinois Department of Labor for six years where he presided over cases dealing with job separation issues and matters pertaining to contested Unemployment Insurance claims. He also co-wrote the agency's administrative rules, and periodically served as a 'ghost writer' for Board of Review decisions. Following that position, he was Director of Development for a Chicago-area non-profit college where he was responsible for High Net Worth donations to the institution. For the next eighteen years he practiced as a solo practitioner attorney with an emphasis in the fields of Real Estate law and Commercial Contracts transactions, and was an agent for several national title insurance agencies.

In 2003 he was recruited to head up a U.S. title insurance research office in Israel, a position he held for four years, and between 2007-2017 he participated in litigation support for several high-profile cases. He has taught Business Law as a faculty member of the Jerusalem College of Technology, and has authored a wide variety of legal White Papers and timely legal articles as a professional legal content writer for GPL clients. Separate from his legal writing, he has co-authored academic articles on Middle East security topics that have been published in peer-reviewed publications.

William H. Anderson, Esq.

MANAGING DIRECTOR AND HEAD OF
FINANCIAL PRODUCTS AND SERVICES

William Anderson is Managing Director and Head of Law & Compliance. He leads the GreenPoint practice in providing regulatory, legal, and technology solutions to law firms, legal publishers, and in-house law departments around the world, overseeing our team of experienced US attorneys and data and technology experts. Will has over 25 years' experience working with corporations to improve the management of their legal and corporate compliance functions. Will began his legal career as a litigator with a predecessor firm to Drinker, Biddle LLP. He then served as in-house counsel to Andersen Consulting LLP, managing risk and working with outside counsel on active litigation involving the firm.

Will has leveraged his legal experience interpreting regulations and appearing before federal (DOJ, SEC, FTC) and state agencies (NYAG) to oversee research and other areas at Bear Stearns. In this capacity, he counseled analysts on regulatory risk and evolving compliance requirements. Will also consulted on the development of a proprietary tool to ensure effective documentation of compliance clearance of research reports. Will then went on to work in product development and content creation for a global online compliance development firm pioneering the dynamic updating of regulated firms' policies and procedures from online updates and resources. Will holds a Juris Doctorate with High Honors from the Washington University School of Law in Saint Louis and is admitted to state and federal bars. He lives in Pawling, NY, with his wife and daughter.

Sanjay Sharma, PhD
FOUNDER AND CHAIRMAN

Pranav Menon, Esq.
LEGAL RECRUITMENT
MANAGER AND DATA
PRIVACY SPECIALIST – LAW
& COMPLIANCE | GPESR

GreenPoint> Law&Compliance

About GreenPoint Law & Compliance

- GreenPoint Global was founded in 2001 and since that time has faithfully served an expanding roster of clients. GreenPoint leverages a unique combination of US-trained attorneys and proprietary technology to deliver a unique offering of skill and flexibility to meet client needs.
- Our core team of experienced US attorneys is based in Israel and works US hours. The breadth of experience of our attorneys ensures high-quality, cost-effective results across a wide range of legal, compliance, and regulatory matters.
- GreenPoint's methodology and proven track record of achieving client objectives has resulted in a broad base of clients in the United States, ranging from Fortune 500 insurance companies to solo practitioners, law firms, in-house law departments, and legal publishers. GreenPoint attorneys are selectively recruited and deployed based on possessing demonstrable subject matter expertise covering a broad spectrum of substantive US laws and regulations. The work product of our attorneys is thoroughly vetted internally before delivery to client. Adherence to quality, value and flexibility is at the core of our foundation.

GreenPoint> Global

About GreenPoint Global

- GreenPoint Global provides litigation support, finance and technology solutions to insurers, law firms, banks, and in-house law departments through our subject matter experts and process specialists.
- Founded in 2001 and headquartered in Rye, New York, GreenPoint has grown to over 500 employees with a global footprint. We have a stable and growing client base that ranges from small and medium-sized organizations to Fortune 1000 companies worldwide. Our production and management teams are located in the US, India, and Israel with access to deep pools of subject matter experts. Our greatest strength is our employee-base of experienced lawyers, paralegals, process specialists, financial analysts, and software developers. We have leading edge software development capabilities with over 50 professionals on staff, working on internal and client projects.
- GreenPoint is certified by the TÜV SÜD (South Asia) for the highest standards of Quality Management (ISO 9001:2015) and Information Security Management (ISO 27001:2013). GreenPoint is certified as a Minority and Woman Owned Business Enterprise (MWBE) by New York City and a Minority Owned Business Enterprise (MBE) by the State of New York. GreenPoint complies with all federal and state contracting requirements. GreenPoint is owned by its founders and principals and is debt free. For comprehensive information on our services and products under Law & Compliance and Finance, please visit our subsidiary websites through the division's menu.