PRIVACY & DATA SECURITY UPDATE 2021:

BILL BUTLER, TANDY MATHIS, AND KARIN MCGINNIS
MOORE & VAN ALLEN, PLLC

September 14, 2021

What Happened in Privacy During the Pandemic (since Nov. 2020)?

- State comprehensive privacy legislation in Virginia and Colorado
- California Privacy Rights Act
- Updates to data breach statutes in Connecticut, Texas and Utah
- New model contractual clauses for cross border transfers under GDPR
- Supreme Court rulings on Computer Fraud and Abuse Act and on Standing
- TCPA rulings.

State Law Data Breach Updates

- **Connecticut (Eff. Oct. 1, 2021)**
  - **Expands definition of personal information** (medical information, a variety of government IDs, health insurance policy or identification numbers, biometric data, and online account information (username and password or security question/answer that would permit access).
  - Data breach **notification timeframe reduced from 90 days to 60 days** (individual and AG)
  - Reporting and notification requirements extended if owns, licenses, or maintains computerized data w/ covered PII even if not do business in Connecticut.
  - The "consultation with law enforcement" language, which was part of the no likelihood of harm carve-out, was removed.

State Law Data Breach Update

Connecticut, ct'd

- **Taxpayer identification number added** as requiring 2 years of identity theft prevention services (along with SSN).
- Investigative documents created in connection with an investigation of a security breach are now **exempted from public disclosure under Connecticut's FOIA.**
- Special notification rules for breaches involving compromised login credentials and to email providers.
- Deemed compliance if HIPAA covered entity and provide notice of HIPAA breach to resident and AG, and provide identity theft protection services if a Social Security or taxpayer identification number are involved.

State Law Data Breach Update

Texas (Eff. Sept. 1, 2021)

- Texas law requires businesses to notify the Texas Attorney General of any data breach affecting at least 250 Texas residents.
- Amendment requires **breach notifications to the Attorney General to include the number of affected residents that have been sent a disclosure by mail or other direct method of communication** at the time of AG notification.
- Amendment also provides that the **Attorney General must update its publicly accessible list** of breach notifications submitted to the AG's office within 30 days of receiving a breach notification report and remove businesses from the list after one year from the notice date.

State Data Security Laws

Currently, at least **24** states have some form of general data security requirement:

- Alabama
- Arkansas
- California
- Colorado
- Connecticut (10/2021)
- Delaware
- Florida
- Illinois
- Indiana
- Kansas
- Louisiana
- Maryland
- Massachusetts
- Minnesota*
- Nebraska
- Nevada
- New Mexico
- New York
- Oregon
- Rhode Island
- Texas
- Utah
- Vermont*
- Virginia (1/2023)

Utah and Connecticut: WISP as Defense to Tort Claims

A. Affirmative defenses under Utah's UCA §§ 78B-4-701 - 78B-4-706 and Connecticut's Public Act No. 21-119 to tort actions alleging failure to implement reasonable information security controls if:

- the covered entity creates, maintains, and complies with a risk based written cybersecurity program containing administrative, technical, and physical safeguards for protection of PI (and restricted information, if applicable), and
- program reasonably conforms to an industry recognized framework (i.e., NIST, ISO 27000, FedRamp, or if already regulated by and comply with federal or state law (GLBA, HIPAA, HiTECH or FISMA), or PCI-DSS+)

Utah and Connecticut Defense to Tort Claims

B. The program must be designed to:

- protect the security and confidentiality of the information;
- protect against any anticipated threats or hazards to the security or integrity of the information; and
- protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud to the individual to whom the information relates.

Comprehensive State Data Privacy Laws

- California Privacy Rights Act (eff. Jan. 1, 2023, applies to data collected after 1/1/22)(amends CCPA)
- Colorado Privacy Act (eff. July 1, 2023)
- Virginia Consumer Data Protection Act (eff. Jan. 1, 2023)

Comprehensive Data Privacy Laws (Cal, Colo and Va)

Law	Coverage	Exclude EE and B2B Data	Eff. Date	Private Cause of Action	Remedies
CCPA	Few entity wide exemptions outside of nonprofits and some HIPAA (but data is exempt) and CMIA regulated entities. No exemption for GLBA regulated entities, but exempts data covered by GLBA. Exempts data subject to FCRA.	X (until 1/1/23)		X lt'd for data brch	
CPRA	Few entity wide exemptions outside of nonprofits and HIPAA and CMIA regulated entities. Exempts data subject to FCRA.		**1/1/23**	Lt'd For Data brch	Enforced by Cal. AG and Cal. Privacy Protection Agency. Penalties and fines up to $2,500 per violation or $7.500 per intentional violation or violation involving consumers under 16. Optional cure/notice period.
CO DPA	1. conducting business in Colorado or targeting residents of Colo. *AND* 2.(a) control or process the personal data of at least **100,000 consumers** in a calendar year, *or* (b) control or process the personal data of at least **25,000 consumers and earn revenue from the sale** of personal data Entity exemptions for GLBA regulated entities and non-profit higher education. Does not exempt (i) non-profits generally and (ii) HIPAA regulated entities, but exempts HIPAA regulated data. Exempts data subject to FCRA.	X	**7/1/23**		Enforced by Colo AG and district attorneys. Violation is treated as deceptive trade practice, subject to up to $20,000 per violation under Col. Consumer Protection Act; but must provide 60 days' notice of a violation and opportunity to cure (if cure is deemed possible). Cure provision expires on 1/1/25.
Va CDPA	1. conducting business in Virginia or who produce products or services targeted to residents of Virginia *AND* 2.(a) control or process the personal data of at least **100,000 consumers** in a calendar year, *or* (b) control or process the personal data of at least **25,000 consumers and derive at least 50% of its gross revenues from the sale** of personal data. Excludes entities subject to GLBA, FCRA and HIPAA. Certain higher ed.	X	**1/1/23**	No	Enforced by Virginia's Attorney General, but must provide 30 days' notice of a violation and opportunity to cure. Damages are limited to up to $7,500 per violation.

Comprehensive Data Privacy Laws
Coverage

Law	Coverage
CCPA	Annual **GR > $25m** or process for commercial purposes **pi of 50,000 consumers/households**, or **50% annual revenues from selling** pi. Few entity wide exemptions. No exemption for GLBA regulated entities, but exempts data covered by GLBA.
CPRA	Same as CCPA except process for commercial purposes **pi of 100,000 consumers/households** and **applies to "sharing" in addition to selling**.
CO PA	Business in CO or targeting residents of CO *AND (i)* control/process the pi of **100,000 consumers** calendar year, *or (ii)* control/process pi of **25,000 consumers and earn revenue from the sale** of pi. Not exempt (i) non-profits generally and (ii) HIPAA regulated entities, but exempts HIPAA regulated data.
Va CDPA	Business in Va or produce products or services targeted to residents of Va *AND* (i) control/process pi **100,000 consumers**/ calendar year, *or* (b) control/ process pi of **25,000 consumers and derive at least 50% of gross revenues from the sale** of personal data. Excludes entities subject to GLBA, FCRA and HIPAA. Certain higher ed.

Comprehensive Data Privacy Laws
Exclude EE and B2B Data

Law	Exclude EE and B2B data
CCPA	X (until 1/1/23)
CPRA	
CO PA	X
Va CDPA	X

Comprehensive Data Privacy Laws
Private Cause of Action

Law	Private Cause of Action
CCPA	X-lt'd for data breach
CPRA	X-lt'd for data breach
CO PA	
Va CDPA	

Comprehensive Data Privacy Laws
Remedies

Law	Remedies
CPRA	Enforced by Cal. AG and Cal. Privacy Protection Agency. Penalties and fines **up to $2,500 per violation or $7,500 per intentional** violation or violation involving consumers under 16. **Optional cure/notice period.**
CO PA	Enforced by Colo AG and district attorneys. Violation is treated as deceptive trade practice, subject to **up to $20,000 per violation under Col. Consumer Protection Act; but must provide 60 days' notice of a violation and opportunity to cure** (if cure is deemed possible). Cure provision expires on 1/1/25.
Va CDPA	Enforced by Virginia's Attorney General, but must provide **30 days' notice of a violation and opportunity to cure.** Damages are limited to **up to $7,500 per violation**.

Customer Rights

Law	Know (Notice, Inc. if Sell)	Access	Correct	Trans-fer (port-ability)	De-lete	Opt-In	Opt-Out	Appeal
CCPA	X	X		X	X - if collected from Consumer		X (sale)	
CPRA	X	X	X	X	X - if collected from Consumer		X (sale or sharing for x - context behavioral advertising)	
CO DPA	X	X	X	X	X - if PD about Consumer	X (sensitive[1] & parental consent for data of < 13 yo (but COPPA data exempt)	X (sale, targeted adv, & profiling on deci. --> legal etc. effects)	X
Va CDPA	X	X	X	X	X - if collected from or about Consumer	X (sensitive[2] & parental consent for data of < 13 yo) [3]	X (sale, targeted adv, [4] & profiling[5] on deci. --> legal etc. effects)	X - If the controller denies the consumer request, it must give the consumer both the reason for the denial and instructions on how to appeal. The appeal rights also must be "conspicuously" set forth in the covered person's privacy policy. Appeals must be processed within 60 days, and if the appeal is denied, the covered person must provide an online or other method for the consumer to contact Virginia's Attorney General to complain.

[1] Sensitive data under the CO DPA includes data revealing race, ethic origin, biometric data, health data, data of a known child.

[2] Va. CDPR defines sensitive data as data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data for uniquely identifying a natural person, data collected from a person known to be a younger than 13 years old, and "precise" geolocation data (locating an individual within a radius of 1,750 feet).

[3] Under Va CDPR, Consent requires an affirmative act showing the consumer's "freely given, specific, informed and unambiguous" consent. Therefore, like GDPR, pre-ticked boxes won't work.

[4] Targeted advertising is specifically defined by the CDPA as covering advertisements displayed to a consumer based on personal data obtained from the consumer over time and across nonaffiliated websites or online applications to predict the consumers preferences or interests. It does not include, however, displaying advertisements based on the consumer's activities on the controller's own website or online applications, search queries, or processing personal data solely for measuring or reporting advertising performance, reach or frequency. The Colo DPA largely follows the Va CDPA definition.

[5] Profiling covers automated processing of personal data to analyze, evaluate or predict a natural person's economic situation, health, personal preferences, interests, reliability, behavior, location or movement. The Colo DPA largely follows the Va CDPA definition.

Customer Rights
Know (Notice, Inc. if Sell)

Law	Know (Notice, Inc. if Sell)
CCPA	X
CPRA	X
CO PA	X
Va CDPA	X

Customer Rights
Access

Law	Access
CCPA	X
CPRA	X
CO PA	X
Va CDPA	X

Customer Rights
Correct

Law	Correct
CCPA	
CPRA	X
CO PA	X
Va CDPA	X

Customer Rights
Transfer (Portability)

Law	Transfer (portability)
CCPA	X
CPRA	X
CO PA	X
Va CDPA	X

Customer Rights
Delete

Law	Delete
CCPA	X - if collected from Consumer
CPRA	X - if collected from Consumer
CO PA	X - if PD about Consumer
Va CDPA	X - if collected from or about consumer

Customer Rights
Opt-in

Law	Opt-In
CCPA	
CPRA	X(sell or share pi of child under 16)
CO PA	X (sensitive[1] & parental consent for data of < 13 yo (but COPPA data exempt)
Va CDPA	X (sensitive[2] & parental consent for data of < 13 yo)[3]

[1] CO PA -- race, ethic origin, biometric data, health data, data of a known child.
[2] Va. CDPR --racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data for uniquely identifying a natural person, data collected from known child (13), and "precise" geolocation data (locating an individual within a radius of 1,750 feet).
[3] Under Va CDPR, Consent requires an affirmative act showing the consumer's "freely given, specific, informed and unambiguous" consent. Therefore, like GDPR, pre-ticked boxes won't work.

Customer Rights
Opt-out

Law	Opt-Out
CCPA	X (sale)
CPRA	X (sale or sharing for x-context behavioral advertising/honor opt out/DNT signals)
CO PA	X (sale, targeted adv, & profiling on decisions ---> legal or similarly sign. effects)
Va CDPA	X (sale, targeted adv,[4] & profiling[5] on decisions ---> legal or similarly sign. effects)

[4] Targeted advertising includes advertisements displayed to a consumer based on personal data obtained from the consumer over time and across nonaffiliated websites or online application, but not advertisements based on the consumer's activities on the controller's own website or online applications, search queries, or processing personal data solely for measuring or reporting advertising performance, reach or frequency.

[5] Profiling covers automated processing of personal data to analyze, evaluate or predict a natural person's economic situation, health, personal preferences, interests, reliability, behavior, location or movement. The Colo DPA largely follows the Va CDPA definition.

Customer Rights
Appeal

Law	Appeal
CCPA	
CPRA	
CO PA	X
Va CDPA	X - If the controller denies the consumer request, it must give the consumer *both* the reason for the denial *and instructions on how to appeal.* The appeal rights also must be "conspicuously" set forth in the covered person's privacy policy. Appeals must be processed within 60 days, and if the appeal is denied, the covered person must provide an online or other method for the consumer to contact Virginia's Attorney General to complain.

Controller Obligations

Law	Data Min.	Pur-pose lts	Data Pro-tection Assess-ment	Privacy Notice	Opt-Out signals	Se-curity Reqs.	Dis-close Sale	Non-discrim
CCPA		X		X	X – DNSMPI	None, but private c/a for harm b/c db	X	X
CPRA	X	X (Consumer also has right to lt use of sensitive data for purpose that goes beyond core purposes permitted by CPRA)	X - for processing that present a significant risk to consumers' privacy or security. (submit to CA Privacy Protection Agency)	X	X – DNSorSMPI	X	X	X
CO DPA	X	X	X - for targeted ads, sales of pd, profiling that creates certain risks, and sensitive data (make avail to CO AG)	X	X - AG to develop	X	X	X
Va CDPA	X	X	X - for targeted ads, sales of pd, profiling that creates certain risks, sensitive data, and other activities that present a heightened risk of harm to consumers.	X		X	X	X

Controller Obligations
Data Minimization

Law	Data Min.
CCPA	
CPRA	X
CO PA	X
Va CDPA	X

Controller Obligations
Purpose Limitations

Law	Purpose Its
CCPA	X
CPRA	X (Consumer also has right to limit use of sensitive data for purpose that goes beyond core purposes permitted by CPRA)
CO PA	X
Va CDPA	X

Controller Obligations
Data Protection Assessment

Law	Data Protection Assessment
CCPA	
CPRA	X – (regulations) for processing that presents a sign. risk to consumers' privacy or security. (submit to CA Privacy Protection Agency)
CO PA	X - for targeted ads, sales of pd, profiling that creates certain risks, and sensitive data (make avail to CO AG)
Va CDPA	X - for targeted ads, sales of pd, profiling that creates certain risks, sensitive data, and other activities that present a heightened risk of harm to consumers.

Controller Obligations
Privacy Notice

Law	Privacy Notice
CCPA	X
CPRA	X
CO PA	X
Va CDPA	X

Controller Obligations
Opt-out Signals

Law	Opt-Out Signals
CCPA	X - DNSMPI
CPRA	X - DNSorSMPI
CO PA	X - AG to develop
Va CDPA	

Controller Obligations
Security Requirements

Law	Security Reqs.
CCPA	None, but private c/a for harm b/c db
CPRA	X
CO PA	X
Va CDPA	X

Controller Obligations
Disclosure of Sale

Law	Disclosure of Sale
CCPA	X
CPRA	X
CO PA	X
Va CDPA	X

Controller Obligations
Nondiscrimination

Law	Nondiscrim
CCPA	X
CPRA	X
CO PA	X
Va CDPA	X

US SUPREME COURT UPDATE

Computer Fraud and Abuse Act

Computer Fraud and Abuse Act: Van Buren v. United States (Oct. 2020).

Held: The CFAA does not impose liability on individuals who use a computer to alter or obtain information they otherwise have authority to access, even when they access the information for a prohibited purpose.

Facts: Police sergeant used patrol car computer to run a license plate number in law enforcement database in exchange for money, in violation of department policy.

Import: "Exceeding authorized access" portion of CFAA prohibition on "intentionally accessing a computer without authorization or exceeds authorized access" references what accessed, not the purpose or use of the access..

TCPA Update

- *Facebook, Inc. v. Duguid* – Automated Dialing Systems
- *TransUnion v. Ramirez* – Standing
- *Fischman v. MediaStratX, LLC* – Private Cause of Action for Internal DNC Requirements

Facebook, Inc. v. Duguid – Automated Dialing Systems

- Facebook sent plaintiff automated security alerts – but Plaintiff never had a Facebook account
- Plaintiff's response: class action lawsuit
  - Violated TCPA by storing numbers and programming equipment to send text messages without consent
- Facebook's defense: its automated system is more advance than TCPA's definition:
  - ATDS: equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers

Facebook, Inc. v. Duguid – Automated Dialing Systems

- Longstanding circuit split over ATDS definition
  - 3rd, 7th and 11th Circuits: must use random or sequential number generation
  - 2nd, 6th and 9th: only needs to store and automatically dial numbers
- 9-0 SCOTUS Decision: narrow definition of ATDS
  - Whether storing or producing numbers, must use random or sequential number generation
  - Under plaintiff's approach, even a cell phone could be an ATDS

Facebook, Inc. v. Duguid – Automated Dialing Systems

- Key takeaways:
  - A win for companies using automated technology to call or text consumers
  - But TCPA litigation is not dead
    - Prerecorded/artificial messages
    - Do Not Call rules
    - State law claims

TransUnion v. Ramirez – Standing

- FCRA class action alleging that TransUnion inaccurately attached national security alerts to credit reports
- Plaintiff alleged two harms:
  1. Failure to maintain reasonable procedures for maximum possible accuracy in consumer reports
  2. Failure to provide consumers with all information in their files
- Class included members whose reports attached inaccurate alerts, but were not disclosed

TransUnion v. Ramirez – Standing

- 9th Circuit: A "material risk of harm" existed sufficient to establish Article III standing
- Supreme Court: "No concrete harm, no standing."
  - 6,332 class members whose reports were not disseminated did not suffer harm
  - Noncompliant format of the mailings were "bare procedural violation[s]"
- TCPA Impact: Is an unwanted message a "concrete harm"?

Fischman v. MediaStratX, LLC – Internal DNC Requirements

- NC federal class action complaint about "extended vehicle warranties"
- Plaintiff alleged violations of TCPA's internal do-not-call requirements (47 C.F.R. § 64.1200(d))
  - Written policy
  - Personnel training
  - Recording & disclosure of DNC requests
  - Identification of sellers and telemarketers
  - Maintenance of internal DNC lists

Fischman v. MediaStratX, LLC – Internal DNC Requirements

- Does 47 C.F.R. § 64.1200(d) create a private cause of action?
  - FCC has not weighed in
  - 6th and 11th Circuits recognize private cause of action
  - Other courts consider them "technical and procedural safeguards"
- E.D.N.C.: "minimum standards" create a private cause of action because they protect privacy rights

GDPR

GDPR-Cross Border Transfers

- Schrems II (last summer)– invalidated Privacy Shield, but also questions SCCs as a legitimate basis for transfers to US.
- EDPB Guidance 1/2020 v.2.0 -- https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
  - Outlines process to ensure transfer adequately protects rights of data subject.
  - Includes process for evaluating laws of country to which data is transferred and "supplementary measures" to protect data if law of country impinges on adequacy of safeguards for transfer in Art. 46 of GDPR.

GDPR Cross Border Transfers

SCCs—new model clauses.

- Different “modules” depending on the roles of the parties (i.e., controller to controller, processor to controller).
- Drafted so that can use in lieu of DPA (don’t need a DPA and the model clauses).
- Non-negotiable.
- Subprocessors can opt-in.
- Include provisions to address EDPB guidance.
- https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

GDPR Cross Border Transfers

- **Immediate:** Use new Model Clauses for any GDPR covered contract where the parties relied on the Privacy Shield for transfer to the US of the EU personal data.
- **September 27, 2021.** Use new Model Clauses for any *new* GDPR covered contract where personal data will be transferred to the US.
- **December 27, 2022.** Use new Model Clauses for any *existing* customer contract that relies on the old Standard Contractual Clauses (SCCs)

ARTIFICIAL INTELLIGENCE

Artificial Intelligence

- Comparison to natural intelligence
- Examples:
  - Targeted advertisements (who will get what ad) *Bradley v. T-Mobile* (ADEA claim b/c ads target younger users)
  - Facial recognition software *FTC v. Everalbum (2020)*(consumer photo-tagging used to develop Ever software)
  - Access to credit or housing *FTC v. RealPage (2018)*(tenant applicant background screening)
  - Criminal justice *State v. Loomis* (predicting recidivism)
  - Employment *Disney (2003*)(CV screening)

What Law Regulates AI?

- Not much!
- FTC guidance **i.e., "Aiming for truth, fairness, and equity in your company's use of AI" Elisa Jillson Apr 19, 2021.**
- State comprehensive privacy laws that address indirectly (profiling) or directly.
- Financial services guidance. https://www.fdic.gov/news/financial-institution-letters/2017/fil17022a.pdf See also https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf
- Case law. AI analyzed under existing laws.

What Law Regulates AI?

More is coming:

- **US:** National Artificial Intelligence Initiative Act of 2020. H.R. Res. 6395, 116th Cong. §§ 5001 et seq. (2020).
- **EU:** Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Act" COM/2021/206 final.
- **Finance:** Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency, *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, 86 FR 16837 (Mar. 31, 2021).

General Principles

- Transparency (notice; possible consent)
- Risk based (financial services, credit, housing, criminal justice, employment, healthcare, essential services)
- Non-discrimination
- Integrity/robustness of underlying data
- Validation and testing
- Impact assessments
- Human intervention (don’t put all your eggs into the AI basket)
- Monitoring
- Security and retention
- Governance (policies, oversight, etc.)

Attorney Contacts

Karin McGinnis
Member
704.331.1078
karinmcginnis@mvalaw.com

Tandy Mathis
Senior Counsel
704.331.2329
tandymathis@mvalaw.com

Bill Butler
Associate
704.331.2455
billbutler@mvalaw.com

Questions?