5 Trends to Watch

January 28, 2021

In celebration of International Data Privacy Day

Nancy Libin, Partner, Washington D.C.

Spencer Persson, Partner, Los Angeles

John Seiver, Of Counsel, Washington D.C.

Kate Berry, Associate, Seattle

Maryam Casbarro, Associate, Washington D.C.

Kara Trowell, Associate, New York

Consumer Privacy

Nancy Libin

Partner, Washington, D.C.

NancyLibin@dwt.com

202.973.4218

Davis Wright Tremaine LLP

Consumer Privacy Legislation 2021: Washington

Washington Privacy Act (the third time may be the charm)

- Elements of GDPR
  - Controllers and processors
  - Consumer rights to access, delete, and correct
  - Data privacy impact assessments
  - Flexible category of “pseudonymous” data
- Elements of CCPA/CPRA
  - Opt-out consent regime, except “sensitive” data used to infer characteristics
  - Opt out of sales, targeted advertising…and profiling
- No private right of action

Consumer Privacy Legislation 2021: Virginia

Consumer Data Protection Act

- Modeled after the WPA
- Roles and responsibilities between “controllers” and “processors” must be memorialized in a contract
  - Provisions similar to GDPR Art. 28 (contractual obligations on processors)
  - Includes obligation to allow and cooperate with assessments of processor’s compliance
  - Requirement to flow down requirements to subcontractors
- Whether entity is a controller or processor is a “fact-based determination”
- Enforcement by Virginia AG – no private right of action…yet

Consumer Privacy Legislation 2021: New York

Biometric Privacy Act (Assembly and Senate)

- Notice to individuals
- No sales of such data
- Limitations on disclosure of such data
- Storage requirements (“reasonable standard of care”)
- Private right of action with liquidated damages

Right to Know Act (Assembly and Senate)

- Consumer right to know and access data
- Private right of action

Data Accountability and Transparency Act (Cuomo)

- Elements of GDPR, CCPA, and CPRA, as well as new provisions
- Enforcement by state regulators, who have rulemaking authority – penalties of up to $7,500/violation

Consumer Privacy Legislation 2021: Other States

Connecticut

- Omnibus consumer privacy bill (notice, access, opt-out of sales, private right of action)
- Children's privacy bill (prohibits collection and commercial use of certain digital information concerning minors)

Minnesota

- CCPA copycat bill with some modifications (no private right of action; enforcement by AG)

New Jersey

- CalOPPA copycat bill that requires websites and online services to post privacy policies, etc.

Oklahoma

- CCPA copycat bill with a private right of action (not limited to data breach) and statutory damages

Consumer Privacy Legislation 2021: U.S. Congress

Consensus around the following issues:

- Require privacy policies to include certain information
- Require opt-in consent to process/transfer “sensitive” information
- Require opt-out consent to process/transfer non-sensitive information to third parties
- Carve out de-identified data and employee data
- Consumer rights (access, delete, and correct)
- Enforcement by FTC and state AGs

Disagreement around:

- Scope of consumer rights, definitions of “covered data” and “sensitive data,” approach to algorithmic bias
- Enforcement – private right of action vs. FTC and state AGs only
- Preemption

State of Play

States

- Actively engaged now – some have short legislative sessions
- Will create compliance challenge if patchwork emerges
- Could be moot if federal legislation preempts state laws

Federal

- Razor-thin margin in Senate and House means compromise necessary
- Additional state laws in 2021 could motivate those on the fence
- Sticking points: private right of action and preemption

Employee Privacy

Kara Trowell

Associate, New York City

KaraTrowell@dwt.com

212-402-4090

Davis Wright Tremaine LLP

Employment Privacy

Many state laws allow access to certain “personnel file” information

- Evaluations
- Performance reviews
- Grievance proceedings
- Records / information relating to promotions, raises, and bonuses
- Payroll records

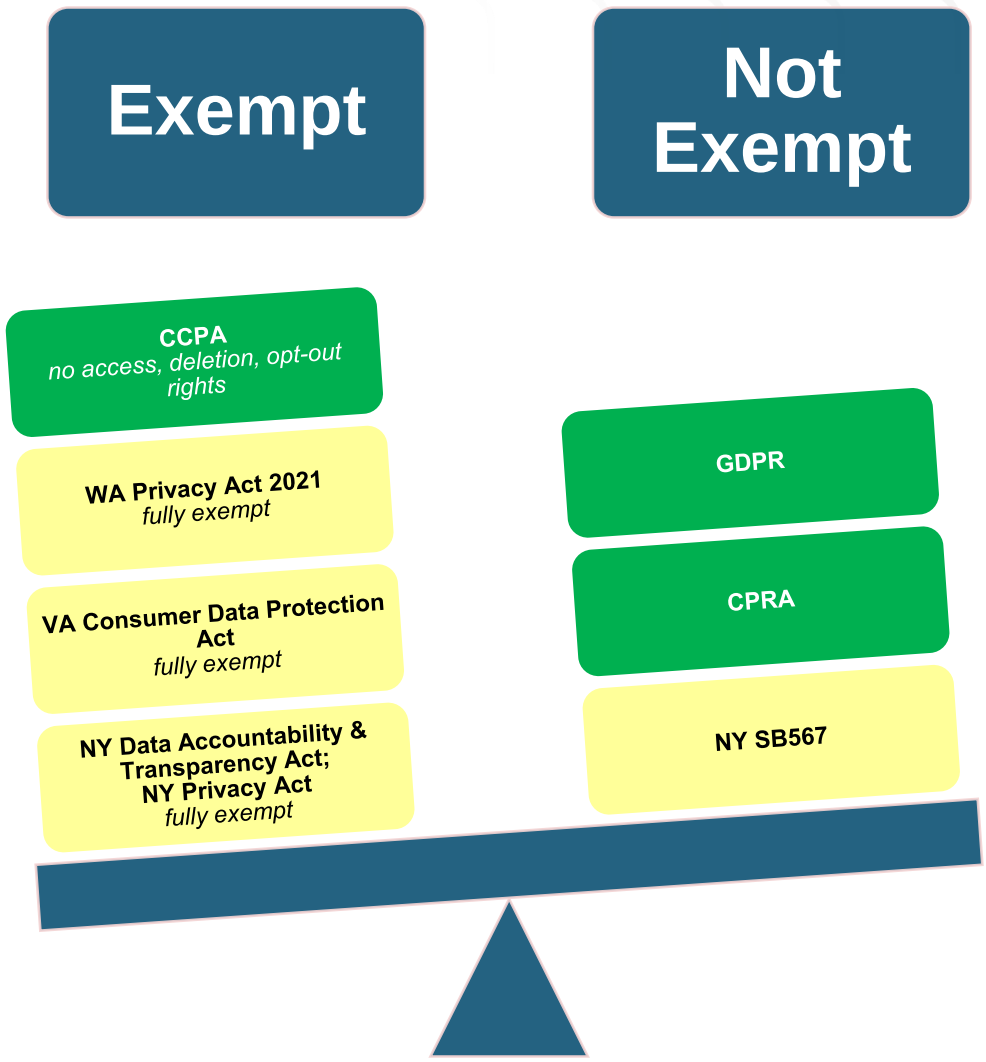
Consumer privacy laws may require that access be provided to a significantly broader scope of employment-related records and information

- Records / information that describe the individual
- Linked geolocation data
- Other information collected to individually monitor and analyze work conduct and performance
- Resumes, cover letters, and other data collected about job applicants
- Work product the individual created or contributed to?
- Communications that mention, were sent to, or received by the individual?

Employment Privacy

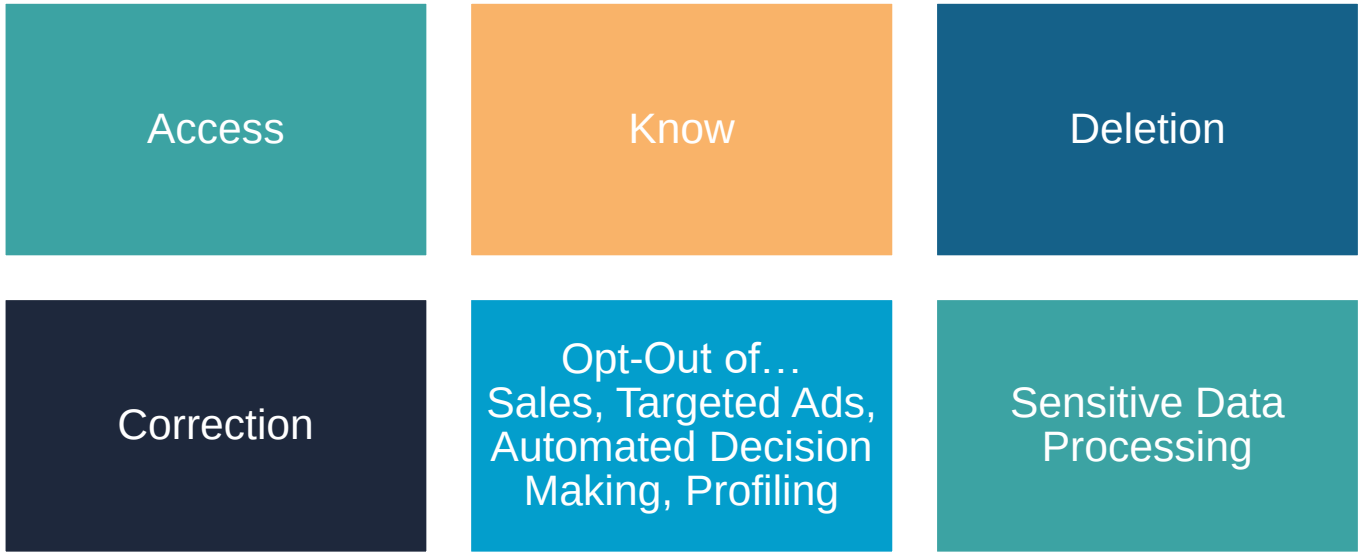
Under enacted and proposed consumer privacy laws:

- No clear trend regarding personnel
- “Employee exemptions” differ in scope and application
  - Which personnel are covered?
  - When does the exemption apply?



Employment Privacy

- Personnel may be able to exercise the full scope of consumer privacy rights



- Businesses will need to **plan and prepare to operationalize privacy rights** for personnel
  - **The California Privacy Rights Act ("CCPA 2.0") will cover personnel as of January 1, 2023!**
    (And apply to data collected about them on or after January 1, 2022)

Facial Recognition & Biometrics

John Seiver

Of Counsel, Washington, D.C.

JohnSeiver@dwt.com

202.973.4212

Kate Berry

Associate, Seattle

KateBerry@dwt.com

206.757.8103

Davis Wright Tremaine LLP

Biometrics

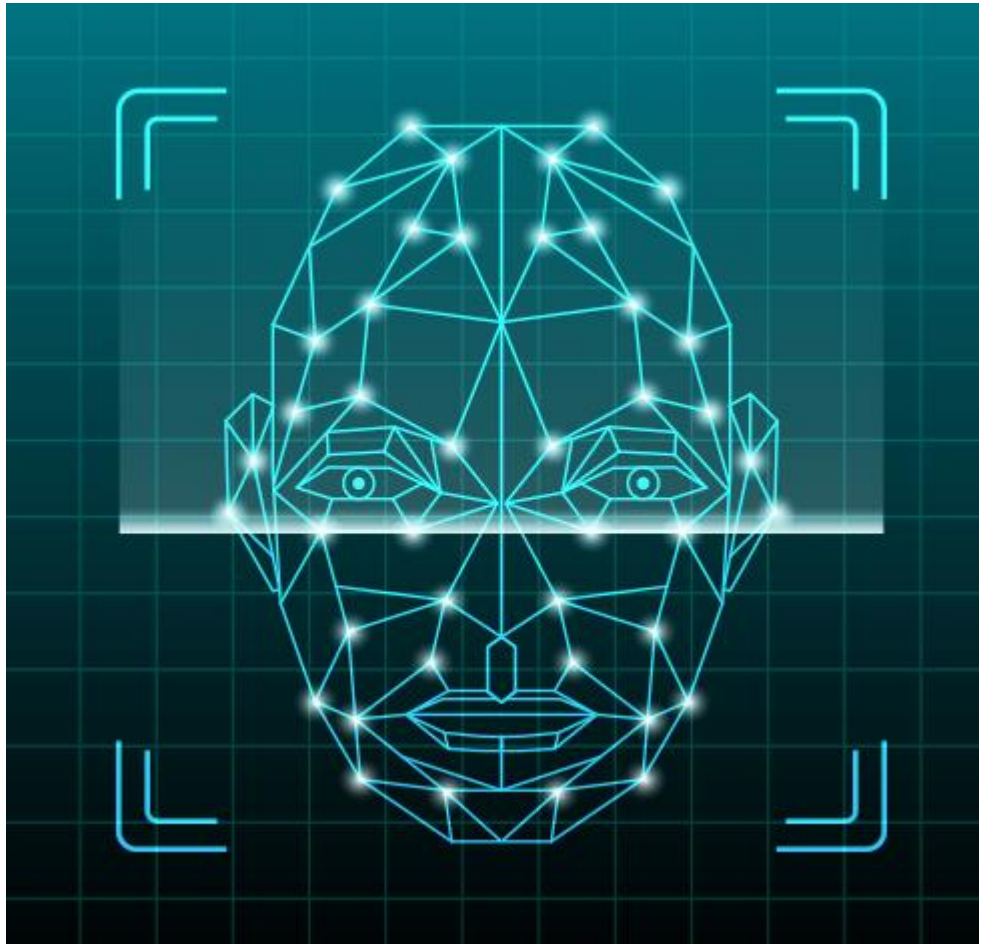
- Biometrics: Characteristics permitting digital identification of a person (e.g., face scans, retinal scan, fingerprints, etc.)
  - Exclusions include photographs
- Biometrics addressed in several states' laws, notably: Illinois, Texas, Washington
  - Obligations of notice, consent, and restrictions on further use
  - IL's private right of action has generated substantial litigation
  - California's CCPA and CPRA also address biometrics
  - At least 19 states restrict use, disclosure, or sharing of biometric data by public or private entities or require security measures

Biometrics: Facial Recognition

- Facial recognition is increasingly a target of regulation
  - Concerns regarding bias, accuracy, and disproportionate effect on minority communities
  - Prohibitions on law enforcement or public officials' use of facial recognition, including in San Francisco; Boston; Portland, OR; Portland, ME; Somerville, MA; Oakland, CA; others
  - Restricted government use: Washington, Oregon, New Hampshire
  - Prohibitions on private business use: Portland, OR
- Some tech companies limiting gov't access to facial recognition technology
- Pending facial recognition proposals in a number of states, Congress
  - Public actors *and* private actors?
  - Ban or limitations? Duration?
  - "Notice and consent"?

Recommendations

- Transparency
- Consider building to BIPA
  - Notice
  - Consent
- Monitor legislative and regulatory developments



Health Information Privacy

Maryam Casbarro

Associate, Washington, DC

MaryamCasbarro@dwt.com

202-973-4268

Davis Wright Tremaine LLP

Trends in Health Information Privacy Law

- M.D. Anderson Fifth Circuit Decision
- Notice of Proposed Rulemaking for Privacy Rule
- HITECH Amendment

M.D. Anderson

Regulatory Encryption Requirement

- Regulation requires only “a mechanism” for encryption
- Does not require:
  - bulletproof protection of “all systems” containing ePHI
  - all ePHI is always and everywhere “inaccessible to unauthorized users”
- Also does not:
  - prohibit asking employees to sign terms as a “mechanism”
  - say providing employees an IronKey is insufficient for compliance
  - say anything about “effectiveness, enforcement, or level of impenetrability”

Definition of Disclosure

- “an affirmative act of disclosure, not a passive loss of information”

Civil Monetary Penalties

- “arbitrary and capricious”

v.

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA
Office for Civil Rights

Notice of Proposed Rule Making

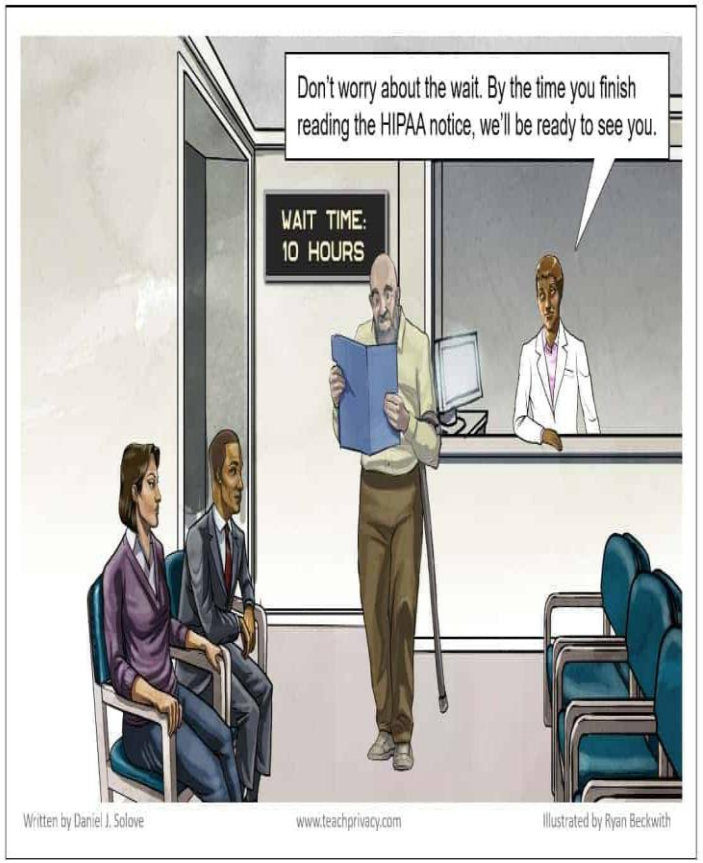
Individuals' Access Rights

"Give it to me straight, doctor. How much longer do I have before you're able to access all of my medical records?"

Coordinated Care

"Relax – we're all in this together."

Notice of Privacy Practices



HITECH Amendment

Secretary to consider whether an entity “has adequately demonstrated that it had, for not less than the previous 12 months, recognized security practices in place that may”:

- mitigate the imposition of fines under section 13410 of the HITECH Act;
- result in the early, favorable termination of an audit under 13411 of the HITECH Act; or
- mitigate remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security Rule between the entity and HHS

“recognized security practices”

“(1) RECOGNIZED SECURITY PRACTICES.—The term ‘recognized security practices’ means the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the covered entity or business associate, consistent with the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title).

Breach Litigation

Spencer Persson

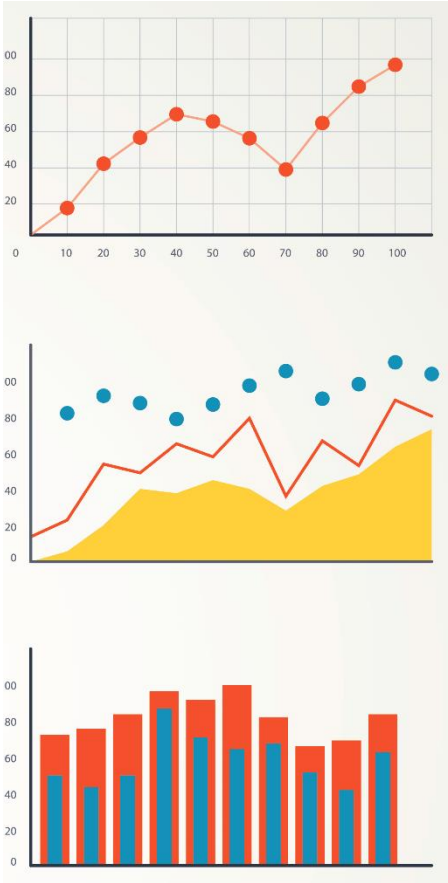
Partner, Los Angeles

SpencerPersson@dwt.com

213.633.8634

Davis Wright Tremaine LLP

Litigation Trends



Civil Privacy Litigation Continues to Focus on Injury, Standing

- Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016): injury-in-fact "requires a plaintiff to allege an injury that is both 'concrete *and* particularized.'"
  - Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017): violation must "actually harm" or at least "actually create a 'material risk of harm.'"
- In subsequent cases, key determinant has been type of information taken and/or whether there is any possibility of identity theft or fraudulent activity.
  - Typically requires exfiltration of SSN, credit or debit card information, driver's license, login and password.
  - Even credit card cases can be dismissed where no fraudulent charges and because card brands likely to reimburse fraudulent charges.

Article III Challenges under CCPA

Will Standing Challenges Apply under CCPA?

- Grant of motion to dismiss in *Rahman v. Marriott*, Case No. 20-cv-00654, Dkt. 34 (C.D. Cal. April 3, 2020).
- Did not address whether CCPA by itself creates an injury sufficient to establish standing.
  - Analogs include BIPA, VPPA, TCPA
- Information allegedly accessed did not fit within CCPA definition of personal information.

- May not apply in state court where no standing requirement.

MTD hearings over next 60 days may provide more guidance.

Open Questions In CCPA Matters

Consumers must provide businesses with a 30-day notice and opportunity to cure before bringing a private right of action for statutory damages

- Many cases are being filed before notice provided, including in *Rahman*; unclear whether claims will be dismissed on procedural grounds

Enforceability of arbitration and class action waiver provisions under Civil Code §§ 1798.150(b) & 1798.192?

- Upcoming in *Atkinson & Renvall v. Minted, Inc.*, Case No. 20-CV-03869

Enforceability of CCPA violations brought pursuant to UDAP/UCL?

Recent Settlements

In re Hanna Andersson and Salesforce.com Data Breach Litigation, Case No. 20-cv-00812 (N.D. Cal. 2020)

- Payment card breach. Included CCPA claim, impacted 200,000 customers
- $400,000 settlement fund, allowing for $5,000 payment if customer has experienced fraudulent charges or $500 if no fraudulent charges; may increase or decrease *pro rata* depending on claims
- Notice paid out of fund; fees and costs up to $120,000

Llamas v. TrueFire, Case No. 20-cv-00857 (M.D. Fla. 2020)

- Payment card breach. Included CCPA claim (but not for statutory damages), impacted 4,911 class members (733 from California)
- Estimated value of $1.2 million, largely tied to complimentary access to music lessons
- All class members eligible for up to $60 in reimbursement payments for time and expenses remediating payment card issues; 733 California class members eligible for separate $50 payment
- Fees and costs up to $156,500