
Morgan Lewis
GLOBAL PRIVACY & CYBERSECURITY 2021 YEAR IN REVIEW AND A LOOK FORWARD TO 2022
January 27, 2022
Pulina Whitaker
Mark Krotoski
Reece Hirsch
Kristin Hadgis
Will Mallin
© 2022 Morgan, Lewis & Bockius LLP

Morgan Lewis

Pulina Whitaker

Mark Krotoski

Reece Hirsch

Kristin Hadgis

Will Mallin

Outline

- Data privacy risks relating to the COVID-19 pandemic
- The European Commission's (EC's) adequacy decisions for the United Kingdom and takeaways from the EC's Standard Contractual Clauses
- Recent rulings including *Lloyd v. Google* and *Warren v. DSG Retail*
- Guidance on the implementation of rules for international transfers
- Outcomes from the UK government's Department for Digital, Culture, Media and Sport's consultation on data protection reform
- The Computer Fraud and Abuse Act following the *Van Buren* decision
- Practices for responding to and preventing ransomware attacks
- Prospects for state and federal privacy legislation in 2022 and preparations for 2023 compliance with new Virginia, Colorado, and California privacy laws

Covid-19 - Privacy Considerations

Privacy obligations are stringent under the UK GDPR and the DPA 2018.

GDPR obligations

The UK GDPR places general obligations on data controllers and processers to ensure lawful processing, transparency of data processing, restricted access to data and the security of data stored by employers. Data cannot be excessive to the lawful purposes.

ICO guidance

Employers must be able to demonstrate that the processing is necessary and cannot be achieved by less intrusive means.

Collecting vaccine status data

Health data is "special category" personal data. Employers must identify both a lawful basis under Article 6(1), and a condition for processing under Article 9, UK GDPR.

Storing personal data

If data is stored in a system, a DPIA may be required. It must be retained for a limited period and deleted when no longer necessary.

Vicarious liability

Where there is a personal data breach by an employee during the ordinary course of their employment, the employer is at risk of being vicariously liable for the breach.

COVID-19: US Privacy Considerations

- The HHS Office for Civil Rights (OCR), which enforces HIPAA, has issued Notifications of Enforcement Discretion loosening certain privacy requirements during the COVID public health emergency
  - Such as permitting telehealth services through "non-public facing" remote communications technologies, such as Zoom or Skype
- Employee COVID testing and vaccination information is not PHI subject to HIPAA
  - But use and disclosure of employee COVID information by an employer may implicate state medical and employment privacy laws
  - Does a disclosure of COVID information violate an employee's reasonable expectation of privacy?

European Commission – Adequacy Decision and SCCs

Adequacy Decision

- The EU Commission published its adequacy decisions in respect of the UK on 28 June 2021.
- Data can therefore flow freely from the EEA into the UK. New arrangements for transfers from the UK to the EEA are not needed.
- The adequacy decision will expire on 27 June 2025 but could in theory end earlier.

EU Standard Contractual Clauses

- On 4 June 2021, the EU Commission issued modernized SCCs for data transfers from controllers/processors in the EU/EEA to controllers/processes established outside the EU/EEA.
- From 27 September 2021, it is no longer possible to conclude contracts incorporating the previous sets of SCCs.
- Until 27 December 2022, organisations can continue to rely on the earlier SCCs for contracts concluded before 27 September 2021.

Recent UK Rulings

Lloyd v. Google

- UK Supreme Court dismissed the first ever "opt-out" class action brought outside of the competition law context.
- Claims for compensation under the Data Protection Act 1998 (**DPA**) cannot proceed on an opt-out basis using the UK's representation action procedure.
- To recover compensation under the DPA, it is not sufficient to prove an infringement of the legislation. Claimants must prove the damages have been suffered as a consequence of the infringement, and "damage" refers to material damage (e.g., financial loss and mental distress).

Recent UK Rulings

Warren v. DSG Retail Ltd.

- DSG suffered a cyber-attack between 2017 and 2018 and was fined £500,000 by the UK's data privacy regulator.
- DSG's systems were accessed by an unauthorised third-party. The Claimant alleged that the cyber-attack compromised his personal data and claimed breaches of the DPA, misuse of private information, and breach of confidence and negligence.
- The UK High Court struck out the claims for compensation for distress for misuse of private information and breach of confidence and negligence.
- The wrong was a "failure" allowing the cyber-attack and not positive conduct by DSG, as required to constitute a breach or misuse for the purpose of breaches of confidence or misuse of private information. These claims do not impose a data security duty on the holders of information.

International Data Transfers

- Restricted transfers from the UK to other countries (which post-Brexit includes the EEA) are subject to transfer rules under the UK regime. Although the UK rules broadly mirror the EU GDPR rules, the UK has independence to keep the framework under review.
- There are currently transitional arrangements which aim to smooth the transition to the new UK regime.
- The continued use of the earlier version of the EU SCCs (valid as at 31 December 2020) is permitted both for existing restricted transfers and for new restricted transfers. The new EU SCCs are not applicable in the UK under the UK GDPR.
- Changes are permitted to these EU SCCs so that they make sense in a UK context provided changes to the legal meaning of the SCCs are not made.
- The ICO has consulted on its own international data transfer agreements (**IDTA**), which will replace the current EU SCCs. We expect the template IDTAs and associated guidance to be published at some point in 2022.

Data protection reform in the UK?

1

What are the proposals?

- The UK Government published its reform proposals in September 2021 – "*Data: a new direction*".
- At a high-level, the proposals for reform are aimed at reducing the tension between increasing innovation and data protection compliance.

2

Data Protection Impact Assessments – abolishment?

- There are proposals to remove the requirement to conduct DPIAs so that organisations and different approaches to identify and minimize data protection risks that better reflect their particular circumstances.

3

Notification of data breaches

- There are also proposals to increase the threshold for reporting data breaches so that no notification is required unless there are material risks to the relevant individuals.

4

Cookies

- The UK government is considering removing consent requirements in connection with analytics cookies to allow for easier consumer profiling and reducing the number of cookie pop-up consent banners.

Morgan Lewis

The Computer Fraud and Abuse Act following the *Van Buren* decision

Computer Fraud and Abuse Act

- Enacted **1984** as the **first federal computer-crime statute**
  - Other statutes often did not apply:
    - Wire fraud
    - Interstate Transportation of Stolen Property
    - Trade Secret Theft
- Five-year statute of limitations

CFAA Provisions

- Obtaining Information
  - § 1030(a)(2)(C)
- Computer Fraud
  - § 1030(a)(4)
- Hacking / Causing Damage
  - § 1030(a)(5)
- Trafficking in Passwords
  - § 1030(a)(6)
- Extortion
  - § 1030(a)(7)
- Department or Agency Computer
  - § 1030(a)(3)
- National Defense or Foreign Relations Information
  - § 1030(a)(1)

Computer Fraud and Abuse Act

- In **1994**, Congress added **civil remedies** to the CFAA under Section 1030(g)
  - "to obtain compensatory damages and injunctive relief or other equitable relief"
- Civil action usually based on "loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value"
  - Other factors may include physical injury, threat to public safety, modification or impairment of "the medical examination, diagnosis, treatment, or care of 1 or more individuals", or damage to a government computer
- Two-year statute of limitations

CFAA Provisions

- Obtaining Information
  - § 1030(a)(2)(C)
- Computer Fraud
  - § 1030(a)(4)
- Hacking / Causing Damage
  - § 1030(a)(5)
- Trafficking in Passwords
  - § 1030(a)(6)
- Extortion
  - § 1030(a)(7)
- Department or Agency Computer
  - § 1030(a)(3)
- National Defense or Foreign Relations Information
  - § 1030(a)(1)

Computer Fraud and Abuse Act

- Section 1030(a)(2)(C): Obtaining Information
  - Prohibits an individual from "intentionally access[ing] a computer **without authorization** or **exceed[ing] authorized access**, and thereby **obtain[ing] … information**" from the computer.

- **"Without authorization"**
  - Undefined
- **"Exceed[ing] authorized access"**
  - "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."

Scope of Insider Access

- How does CFAA apply to insiders who "exceed authorized access" to computer information?
  - Distinguish external access "without authorization" (e.g., hackers).

- "Faithless employee"
  - "'[S]o-called faithless or disloyal employee' — that is, an employee who has been granted access to an employer's computer and misuses that access, either by violating the terms of use or by breaching a duty of loyalty to the employer." *Chefs Diet Acquisition Corp. v. Lean Chefs* , LLC, 2016 WL 5416498, *6 (SDNY 2016)

- Circuit Split
  - Whether an insider or employee acting with the intent to steal the company's information or with an improper purpose with the company's computer violates the CFAA.

CFAA Circuit Split

Broad

- **First Circuit***: EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st 2001) (contrary to non-disclosure and use terms)
- **Seventh Circuit***: Int'l Airport Centers v. Citrin*, 440 F.3d. 418, 420-21 (7th Cir. 2006) ('breach of "duty of loyalty" terminates "authority to access" under the CFAA)
- **Fifth Circuit***: United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010) ("authorized access" can encompass use limits, "at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.")
- **Eleventh Circuit***: United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (CFAA covers access of personal records for nonbusiness reasons)

Narrow

- **Ninth Circuit***: United States v. Nosal*, 676 F.3d. 854, 863 (9th Cir. 2012) (en banc)
- **Fourth Circuit***: WEC Carolina Energy Solutions v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (adopting "a narrow reading" under the CFAA)
- **Second Circuit***: United States v. Valle*, 807 F.3d 508 (2d Cir. 2015)

Circuit Split on Similar Facts

- **Second Circuit***: United States v. Valle*, 807 F.3d 508 (2d Cir. 2015)
  - New York City Police Department officer used law enforcement database to obtain information about one of his former high school classmates so that he could engage in a fantasy role-play kidnapping scenario.
  - **Trial conviction.**
  - **Reversed on appeal**.

Circuit Split on Similar Facts

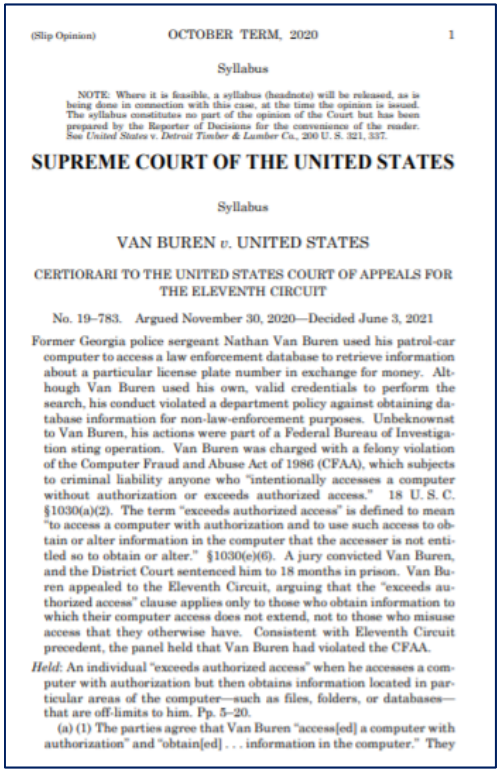
- **Second Circuit***: United States v. Valle*, 807 F.3d 508 (2d Cir. 2015)
  - New York City Police Department officer used law enforcement database to obtain information about one of his former high school classmates so that he could engage in a fantasy role-play kidnapping scenario.
  - **Trial conviction.**
  - **Reversed on appeal**.

- **Eleventh Circuit***: United States v. Van Buren*, 940 F.3d 1192, 1208 (11th Cir. 2019)
  - Georgia police sergeant accessed a law enforcement database to obtain information about a license plate number in exchange for money.
  - **Trial conviction.**
  - **Affirmed on appeal**.

Van Buren Question Presented

- "Whether a person who is **authorized to access** information on a computer **for certain purposes** violates Section 1030(a)(2) of the Computer Fraud and Abuse Act [to obtain information from a protected computer] if he **accesses the same information for an improper purpose**." *Van Buren v. United States*, No. 19-783 (April 2020).

- ***Van Buren v. United States*, 141 S.Ct. 1648 (June 3, 2021)**



(Slip Opinion) OCTOBER TERM, 2020 1

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

VAN BUREN *v.* UNITED STATES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

No. 19–783. Argued November 30, 2020—Decided June 3, 2021

Former Georgia police sergeant Nathan Van Buren used his patrol-car computer to access a law enforcement database to retrieve information about a particular license plate number in exchange for money. Although Van Buren used his own, valid credentials to perform the search, his conduct violated a department policy against obtaining database information for non-law-enforcement purposes. Unbeknownst to Van Buren, his actions were part of a Federal Bureau of Investigation sting operation. Van Buren was charged with a felony violation of the Computer Fraud and Abuse Act of 1986 (CFAA), which subjects to criminal liability anyone who "intentionally accesses a computer without authorization or exceeds authorized access." 18 U. S. C. §1030(a)(2). The term "exceeds authorized access" is defined to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." §1030(e)(6). A jury convicted Van Buren, and the District Court sentenced him to 18 months in prison. Van Buren appealed to the Eleventh Circuit, arguing that the "exceeds authorized access" clause applies only to those who obtain information to which their computer access does not extend, not to those who misuse access that they otherwise have. Consistent with Eleventh Circuit precedent, the panel held that Van Buren had violated the CFAA.

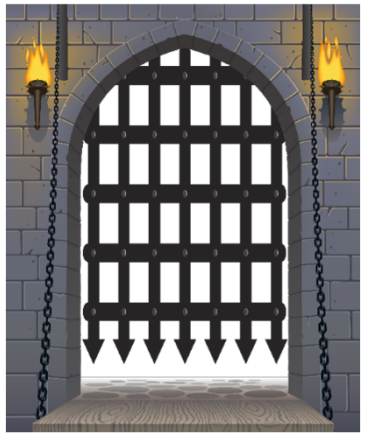
Held: An individual "exceeds authorized access" when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to him. Pp. 5–20.

(a) (1) The parties agree that Van Buren "access[ed] a computer with authorization" and "obtain[ed] . . . information in the computer." They

https://www.supremecourt.gov/qp/19-00783qp.pdf

Van Buren

- "Under Van Buren's reading, liability under both clauses [of the CFAA concerning access "without authorization" or "exceeds authorized access"] stems from a **gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system**. And reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry." *Van Buren*, 141 S.Ct. at 1658-59.



Van Buren

- "In the computing context, 'access' references the act of **entering a computer 'system** itself' or a particular '**part of a computer system**,' such as **files, folders, or databases**. It is thus consistent with that meaning to equate 'exceed[ing] authorized access' with the act of entering a part of the system to which a computer **user lacks access privileges**." *Van Buren*, 141 S.Ct. at 1657-58.

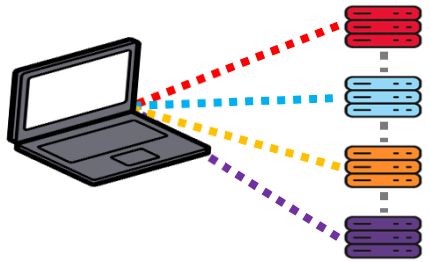
- "In sum, an individual **'exceeds authorized access'** when he accesses a computer with authorization but then **obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him**." *Van Buren*, 141 S.Ct. at 1662.
- "Van Buren accordingly did not 'excee[d] authorized access' to the database, as the CFAA defines that phrase, even though he obtained information from the database for an improper purpose." *Id*.

After *Van Buren*

- Recurring "insider scenario"
  - Remedy for theft or misuse of information
  - "Faithless" or "Disloyal Employee"

- After *Van Buren*, clearly restrict access to particular "files, folders, or databases"

- Other options
  - Trade secret remedies
  - Confidential Information Agreements
  - Exit Interview



- Eventual congressional action?
  - Time to modernize the CFAA?

Morgan Lewis

Ransomware Attacks and Current Developments

Ransomware Attacks – What Are They?

- The increase in ransomware attacks is the big news in privacy and cyber fields.
- 700% increase in ransomware attacks for 2020, even more in 2021.
- What are they?
  - Threat actor enters system and uses malware to encrypt the system to shut it down
  - Provides a ransom note demanding payment in cryptocurrency in exchange for the key needed to decrypt the system
  - Launched by organized criminal groups, typically located in Russia, China, or North Korea, with Darkside, Nightwalker, and Revil.
  - Dual threat—exfiltration of sensitive data

Ransomware Attacks – What Is Causing Them?

- Change in business model—traditional attacks focused on exfiltration are more difficult to perpetrate and less lucrative.
  - Companies avoid storing sensitive data, use encryption, use multi-factor
  - Payment network has evolved with chip technology and other changes
  - Your data is already out there!
- Fueled by the rise in remote work and distraction due to COVID-19 over the last year, which has opened companies to more vulnerability.
  - Use of remote access tools, such as outdated VPNs and equipment, personal devices, unsecure Wi-Fi
  - Microsoft found that the level of overall cyber attacks reached an all-time high in the three months immediately after WHO announced that COVID-19 was a global pandemic in May 2020.

Ransomware Attacks – How to Respond When They Occur?

- Convene the incident response team
- Outside counsel's role
- Outside cybersecurity expertise
- Insurance
- PR and crisis communications
- Contacting law enforcement
- Negotiating a ransom payment
- Data mining
- Notification obligations

Ransomware Attacks – Is It Alright to Pay?

- US Department of the Treasury's Office of Foreign Assets Control (OFAC) recently issued an updated advisory on potential sanctions risks for companies facilitating payments in connection with ransomware attacks.
- In September 2021, OFAC for the first time sanctioned a cryptocurrency exchange for its part in facilitating financial transactions for ransomware actors, and it will continue to impose sanctions on those who provide financial, material, or technological support for ransomware activities.
- Violations of OFAC regulations may result in civil penalties based on strict liability.
- OFAC strongly discourages companies from making ransomware payments and instead recommends focusing on strengthening defensive measures and reporting to/cooperating with authorities—actions that OFAC would consider to be "mitigating factors" in any related enforcement action.

Ransomware Attacks – How Can You Prevent Them?

- Focus on backups—ensure regular, complete, and segregated.
- Know your system and endpoints—inventory and data map are critical.
- Consider vulnerabilities created in remote work environment.
- Maintain good, consistent cyber hygiene
  - Regular patches
  - Updated anti-virus
  - Authentication protocols (passwords and multi-factor)
- The buck stops with your incident response team and planning process.

Morgan Lewis

US Federal & State Privacy Law Developments

Prospects for Federal Privacy Legislation

- The chances for passage of a comprehensive federal privacy law in 2022 are slim
  - Focus will be on midterm elections
  - If the Republicans gain a majority in the House or Senate in the midterms, privacy legislation is less likely to move in a divided government
- Preemption of state privacy laws and the availability of a private right of action remain sticking points
- However, the pressure continues to build as states such as CA, VA, and CO pass their own privacy laws
- On January 13, the US Chamber of Commerce and a host of business organizations delivered a letter to Congress, pleading for federal privacy legislation to counter a "growing patchwork of state laws" that "threaten innovation and create consumer and business confusion"

California Consumer Privacy Rights Act (CPRA)

CPRA "CCPA 2.0" Ballot Initiative Passed on Nov. 3, 2020 (effective Jan. 2023, with enforcement commencing July 1, 2023)

- Adds protections for "sensitive personal information"
- Adds right to opt out of "sharing" of data, not just "selling" of data
- Adds right to opt out of cross-context behavioral advertising
- Adds the right to correct inaccurate PI
- CCPA's partial exceptions for employees, applicants, officers, directors, contractors, and business representatives extended through January 1, 2023
- Extends lookback period for requests to know beyond 12 months

California Privacy Protection Agency

- **The CPRA creates a new enforcement agency: California Privacy Protection Agency**
  - The Agency will assume the California AG's responsibility for interpreting and enforcing CCPA/CPRA
  - The Agency will consist of a 5-member board.
    - Members may not serve longer than 8 consecutive years
- The functions of the agency will include:
  - Implementation and enforcement of the CPRA
  - Adopting CPRA regulations
  - Providing guidance to businesses and consumers regarding the CPRA
  - Issuing orders that require violators to pay administrative fines of up to $2,500 per violation of the Act or up to $7,500 per intentional violation
- AG will retain authority to go to court to enforce the CPRA

CCPA Developments

- In October, CPPA hired an executive director – Ashkan Soltani, a former FTC chief technologist
- Passage of AB 694 clarifies the deadline for issuance of CPRA regulations by the CPPA
  - Effect is that CPPA could issue rules around April 19, 2022
- At a November meeting, the CPPA considered the following responses to rulemaking challenges
  - Engaging in emergency rulemaking to write rules faster than the standard timeline
  - Delaying enforcement of the CPRA
  - Hiring temporary staff
  - Staggering rulemaking, which could impact companies' compliance programs and timing

Sensitive Personal Information

- CPRA defines "sensitive personal information" (SPI) to include account and login information; precise geolocation data; contents of mail, email, and text messages; genetic data; and certain sexual orientation, health, and biometric information
- A consumer has the right to direct a business that collects SPI to limit its use of the consumer's SPI to uses necessary to perform the services or provide the goods
  - As reasonably expected by an average consumer
- If a business uses or discloses SPI for other purposes, the consumer must be given right to opt out of those uses or disclosures of SPI
- However, if SPI is collected "without the purpose of inferring characteristics about a consumer" it can be treated as "personal information"
  - Businesses need to carefully consider whether SPI is being collected for consumer profiling purposes, or whether collection is incidental to services
  - Standard will be clarified through future regulations

Sensitive Personal Information Opt-Out

- Business must provide a "Limit the Use of My Sensitive Personal Information" link on its homepage
- Consumer must be given the option to restrict uses and disclosures of SPI to what is reasonably necessary to provide goods and services
- Similar to GDPR concept
- Virginia Consumer Data Protection Act also includes similar provision regarding sensitive information
  - Significantly, requires opt-in, rather than opt-out
- If a national company adopts a more stringent opt-in approach to SPI, would that satisfy CPRA?
  - Unclear at this time, but appears that a bifurcated compliance approach for CA and VA would be needed

Behavioral Advertising Opt-Out

- CPRA expands consumer right to opt-out to include "sharing" as well as "sale"
- New definition of "sharing" includes sharing, renting, transferring or communicating PI to a third party for "cross-context behavioral advertising"
  - Whether or not for monetary or other valuable consideration
- "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or other services
  - OTHER THAN the business, distinctly branded website, application, or service with which the consumer intentionally interacts

Other New CPRA Requirements

- Adds requirements for businesses to protect PI
  - Minimizing data collection
  - Limiting data retention
  - Protecting data security
  - Privacy risk assessments and cybersecurity audits
- Expands the private right of action to cover (1) nonredacted and nonencrypted information; ***and*** (2) email addresses with a password or security question and answer that would permit access to the account (*this second category is new*)
  - **NEW:** Security measures implemented after a breach do not constitute a cure of that breach

Virginia's Consumer Data Protection Act (CDPA)

- Virginia's privacy law will go into effect on January 1, 2023
- The act will apply to businesses that
  - Operate in Virginia or produce products or services that are targeted to Virginia residents and that either:
    - Control or process the personal data of at least 100,000 Virginia residents during a calendar year, or
    - Control or process the personal data of at least 25,000 Virginia residents and derive at least 50% of its gross revenue from the sale of personal data
- Applies to brick-and-mortar businesses, not just the collection of personal data electronically or over the internet
- Does not apply to employment-related data or B2B transaction data

Virginia Privacy Rights Overview

- Right to access personal data
- Right to correct inaccuracies in personal data
- Right to delete personal data
- Right to data portability
- Right to opt out of the sale of personal data
- Consumer right to appeal a controller's response to a consumer request

Enforcement of Virginia's Privacy Law

- There is no private right of action under the CDPA (even for data breaches)
- The VA Attorney General will have exclusive authority to enforce the CDPA, subject to a 30-day cure period
- Violators are subject to civil penalties of up to $7,500 for each violation

The Colorado Privacy Act (CPA)

- Colorado's privacy law will go into effect on July 1, 2023
- The act will apply to businesses that
  - Conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to residents of Colorado and:
    - Control or process the personal data of at least 100,000 Colorado residents during a calendar year, or
    - Derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of 25,000 consumers or more.
- Grants Attorney General rulemaking powers
- Does not apply to employment-related data or B2B transaction data

Colorado Privacy Rights Overview

- Right to access personal data
- Right to correct inaccuracies in personal data
- Right to delete personal data
- Right to data portability
- Right to opt out of the sale of personal data
- Consumer right to appeal a controller's response to a consumer request

Enforcement of Colorado's Privacy Law

- There is no private right of action under the CPA
- Provides for broad enforcement authority to the CO Attorney General and District Attorneys, subject to a 60-day cure period
- Violators are subject to civil penalties of up to $20,000 for each violation

Virginia and Colorado: Sensitive Data Opt-In

- The laws in Virginia and Colorado prohibit processing of sensitive data without first obtaining the consumer's consent
  - "Sensitive data" includes (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status, (2) processing of genetic or biometric data for the purpose of uniquely identifying a person, (3) personal data collected from a known child, and (4) precise geolocation data (VA only)
  - "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data

- The CPRA contains no comparable opt-in requirement
- Consumers have the right to limit the use of their sensitive personal information by submitting a request to a business under the CPRA

Data Subject Rights

DATA SUBJECT RIGHTS	VA CDPA	CO CPA	CA CCPA	CA CPRA
Access	Yes	Yes	Yes	Yes
Correct	Yes	Yes	No	Yes
Delete	Yes (data provided by or obtained about consumer)	Yes (data concerning the consumer)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes	Yes
Opt-Out of Sale	Yes	Yes	Yes	Yes
Opt-Out of Sharing	No	No	No	Yes
Non-Discrimination	Yes	Yes	Yes	Yes
Appeals Process	Yes	Yes	No	No

Controller Obligations

Controller Obligations	VA CDPA	CO CPA	CA CCPA	CA CPRA
Data Minimization	Yes	Yes	No	Yes
Purpose Limitation	Yes	Yes	Yes	Yes
Security Requirements	Yes	Yes	No	Yes
Special Requirements for Children's Data	Yes (sensitive data of children under 13 years of age)	Yes (sensitive data of children under 13 years of age)	Yes (sale of PI of children under 16 and 13 years of age)	Yes (sale of PI of children under 16 and 13 years of age)
Privacy Notice	Yes	Yes	Yes	Yes
Data Protection Assessment	Yes	Yes	No	Yes – submitted to the CA Privacy Protection Agency

Practical Compliance and What's Next in State Privacy Legislation?

- Compliance Considerations
  - January 1, 2023 is now less than one year away.
  - Use the runway available – try things out.
  - Recognize the landscape may change, including with any rules or regulations that may come, so do not finalize until mid-to-late 2022.
  - Educate leadership about how this will evolve.
  - Invest in teams and technology to be able to scale up on requests.
- In 2021, nearly a dozen states were actively debating a comprehensive privacy law
  - Debate, however, does not guarantee that a law will pass
  - The Washington Privacy Act bill failed for the third straight year
  - Many states, however, have introduced bills. Stay tuned…

Questions?

Morgan Lewis

PULINA WHITAKER

Pulina Whitaker
London
+44.20.3201.5550
pulina.whitaker@morganlewis.com

Pulina Whitaker's practice encompasses data privacy and cybersecurity as well as employment matters. Co-head of the firm's global privacy and cybersecurity practice, she manages employment and data privacy issues on an advisory basis and in sales and acquisitions, commercial outsourcings, and restructurings. Pulina manages international employee misconduct investigations as well as cross-border data breach investigations. She has been appointed as a compliance monitor for the United Nations and for USAID. She is also a trustee of Hostage International. She acts for employers in defending against employment and data privacy allegations and claims, including for bullying/harassment, unfair dismissal, discrimination, whistleblowing, breach of data processing, and employment contract claims. She has experience working with international and European clients to help them comply with the EU General Data Protection Regulation, including advising on audits of data processing activities and data security incidents.

MARK L. KROTOSKI

Mark L. Krotoski
Silicon Valley
Washington DC
+1.650.843.7212
+1.202.739.5024
mark.krotoski@morganlewis.com

Litigation Partner, Privacy and Cybersecurity and Antitrust practices

- Co-Head of Privacy and Cybersecurity Practice
- Litigates, responds to a data breach, directs confidential cybersecurity investigations, responds to federal and state regulatory investigations, coordinates with law enforcement on cybercrime issues, mitigates and addresses cyber risks, and develops cybersecurity protection plans.
- 25 years' experience handling a broad range of complex and novel cyber cases and investigations under the Computer Fraud and Abuse Act, Economic Espionage Act, Defend Trade Secrets Act, and other statutes.
- Served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, in addition to other DOJ leadership positions.

W. REECE HIRSCH

W. Reece Hirsch
San Francisco
+1.415.442.1422
reece.hirsch@morganlewis.com

W. Reece Hirsch co-heads the firm's privacy and cybersecurity practice and counsels clients on a wide range of US privacy issues, specializing in healthcare privacy and digital health. Reece counsels clients on development of privacy policies, procedures and compliance programs, security incident planning and response, and online, mobile app, and Internet of Things privacy. Reece counsels clients in healthcare privacy and security matters, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, state medical privacy laws, and Federal Trade Commission standards applicable to digital health companies. He has represented clients from all sectors of the healthcare industry on privacy and security compliance, including health plans, insurers, hospitals, physician organizations, and healthcare information technology, digital health, pharmaceutical, and biotech companies. Reece also advises clients on privacy issues raised by the coronavirus (COVID-19) pandemic, including those relating to workplace testing, HIPAA waivers and enforcement discretion, contact tracing, telehealth, and work-from-home and return-to-work policies.

KRISTIN M. HADGIS

Kristin M. Hadgis
Philadelphia
+1.215.963.5563
kristin.hadgis@morganlewis.com

Kristin M. Hadgis counsels and defends retail and other consumer-facing companies in matters relating to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, retail operations, loyalty and gift card programs, and commercial disputes. Kristin also handles data security incident response crisis management, including any resulting litigation or government investigations.

Kristin has advised on more than 250 data breaches in her career, counseling clients on how best to give notice to affected individuals or government and consumer reporting entities, following proper compliance protocol. Kristin also represents these companies on any class action and other litigation stemming from the incidents, and instructs them on implementing policies and procedures to prevent and mitigate future breaches.

WILLIAM MALLIN

William Mallin
London
+44.20.3201.5374
william.mallin@morganlewis.com

Will Mallin advises clients on a range of contentious and non-contentious employment matters in addition to employment aspects of corporate transactions. He has experience in dismissals, redundancies, discrimination, internal investigations, grievances, disciplinaries, and Employment Tribunal proceedings. He also has experience acting on data privacy matters and in advising clients on the employment law related aspects of the COVID-19 pandemic. Will completed his training contract at Morgan Lewis gaining experience across the firm's labor and employment, corporate, antitrust, and litigation departments.

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

Morgan Lewis

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.

THANK YOU