


HUSCHBLACKWELL


Analyzing the Colorado Privacy Act Final Rules

—

David M. Stauss, Partner, CIPP/US/E, CIPT, FIP, PLS



1



Roadmap

1. Takeaways
2. Quick Recap of CPA
3. Consumer Requests
4. Universal Opt-Out Mechanism
5. Privacy Notices
6. Other Processing Requirements
7. Loyalty Programs
8. Sensitive Data
9. Consent
10. UI Design, Choice Architecture, and Dark Patterns
11. Data Protection Assessments
12. Profiling

HUSCHBLACKWELL

© 2023 Husch Blackwell LLP

2

Takeaways

© 2023 Husch Blackwell LLP

3



Takeaways

1. Rules effective July 1, 2023 (same date as statute)
2. Extensive changes from draft rules (mostly pro-business)
3. Specific attention needs to be spent on requirements for sensitive data inferences, privacy notices, processing purposes, secondary uses, data minimization and retention, data protection assessments, and profiling

HUSCHBLACKWELL

© 2023 Husch Blackwell LLP

4

Quick Recap of CPA

© 2023 Husch Blackwell LLP

5



Scope

Controller that conducts business in Colorado or produces or delivers commercial products or services that are intentionally targeted to Colorado residents



100,000

“controls or processes the personal data of” 100,000 “consumers or more during a calendar year”

OR

Sell + 25,000

“derives revenue or receives a discount on the price of goods or services from the sale of personal data of” 25,000 “consumers or more”

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

6

H-B

Exemptions



GLBA financial institutions and data



PHI collected by covered entities and business associates, and numerous other healthcare-related exemptions



Certain data maintained by state



Certain data maintained by public utilities



Certain FCRA data



Data maintained for employment records purposes



Air carrier as defined in regulations



Data subject to Driver's Privacy Protection Act



Data regulated by COPPA

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

Obligations

Rights

- Access, delete, portability, correct, confirm processing, opt out of targeted advertising, sales and certain types of profiling

Privacy policy

Sensitive data

- Must obtain consent to process

Data protection assessments

- Must complete for high-risk processing activities

Data processing agreements

- Rules do not address

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP



CPA Resource Center

☰ MENU **HUSCH BLACKWELL**



Capabilities / Colorado Privacy Act Resource Center

Colorado Privacy Act Resource Center

Helping companies navigate and comply with Colorado's consumer privacy legislation.

On July 7, 2021, Colorado officially became the third state – after California and Virginia – to pass broad consumer privacy legislation when Governor Jared Polis signed the [Colorado Privacy Act \(CPA\)](#) into law. The CPA will go into effect on July 1, 2023.

Key Contact
 **David M. Stauss**
 Partner

[View our entire team >](#)
[Download Service >](#)

[READ THE BLOG POSTS >](#)
[VIEW THE WEBINARS >](#)

Overview
 Thought Leadership - Insights
 Events
 News

Related areas of focus:
[California Consumer Privacy Act >](#)
[Data Privacy & Cybersecurity >](#)
[State Privacy Laws >](#)



HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

9

Consumer Requests

© 2023 Husch Blackwell LLP

10



Methods for Receiving Requests

Privacy Notice

- Methods must be specified in privacy notice

Two Designated Methods

- Unless controller operates exclusively online (see below) it must offer two or more methods
- If controller has a website, app, or other digital presence, one method has to be through website, app, or digital interface such as through a webform

Controller Operates Exclusively Online

- If a controller operates exclusively online and has direct relationship with consumer it can use email address for access, correction, deletion, and portability requests

In Person

- “Shall consider providing an in-person method” if controller interacts with consumer in person

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

11



Methods for Receiving Requests

Does not need to be Colorado specific if method:

- Clearly indicates which rights are available to Colorado consumers
- Provides all data rights to Colorado consumers
- Provides Colorado consumers with clear understanding of how to exercise their rights
- Otherwise complies with regulations

Accounts

- Cannot require consumers to create a new account but can require consumers to use existing password-protected account

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

12

Response



Timing

45 days (unchanged from statute)
 Requests to opt out must be processed “as soon as feasibly possible and without undue delay”



Denial

If controller denies request, then it must explain basis for denial and provide instructions for how to appeal





Authentication

Rules are not prescriptive like California’s requirements

Need to use “commercially reasonable method” for authentication



Commercially Reasonable Factors

-  Data right exercised
-  Type, sensitivity, value, and volume of personal data
-  Level of possible harm that improper access or use could cause
-  Cost of authentication

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

15

Right to Opt Out

© 2023 Husch Blackwell LLP

16

Right to Opt Out

- Sales / Targeted Advertising**
 - Must provide an opt-out method either directly or through a link, in a clear, conspicuous, and readily accessible location outside privacy notice
- Profiling**
 - Must provide a clear and conspicuous method at or before the time profiling occurs

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

17

If link is used it must:

- 01**
Comply with Rule 4.02(B)
• E.g., enable a consumer to submit the request at any time; be easy to execute
- 02**
Take consumer directly to opt-out method
- 03**
Provide clear understanding of purpose
• E.g., "Colorado Opt-Out Rights," "Personal Data Use Opt-Out," "Your Opt-Out Rights," "Your Privacy Choices," "Your Colorado Privacy Choices"

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

18

Link Text

Colorado

Any clear and conspicuous method for Consumers to exercise the right to opt out of Processing for the Opt-Out Purposes, provided pursuant to this section, must comply with the requirements of 4 CCR 904-3, Rule 4.02(B). If a link is used, it must take a Consumer directly to the opt-out method and the link text must provide a clear understanding of its purpose, for example "Colorado Opt-Out Rights," "Personal Data Use Opt-Out," "Your Opt-Out Rights," "Your Privacy Choices," or "Your Colorado Privacy Choices."

California

(b) A business that chooses to use an Alternative Opt-out Link shall title the link, "Your Privacy Choices" or "Your California Privacy Choices," and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business's internet Homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.



HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

19

Other Rights

© 2023 Husch Blackwell LLP

20



Right of Access



Specific Pieces

Must respond with all specific pieces of personal data collected and maintained about consumer, including personal data obtained by processors



Format

Provide data in concise, transparent and easily intelligible form that avoids "incomprehensible internal codes"



Data Breach Protections

Not required to disclose sensitive information such as SSNs and passwords but need to explain that controller has collected that information

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

Right to Correction

Process

- Must correct personal data in existing systems, except archive or backup systems, and instruct processors to make necessary corrections in their systems
- Controller can delay compliance for personal data stored on archived or backup systems until they are restored or is next accessed or used

Account Settings

- Can direct consumers to account settings to make corrections under certain circumstances

Standard

- Controller can require consumers to provide documentation
- Controller can decide not to act if it determines that contested personal data is more likely than not accurate

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

Right to Deletion

Controller must

- Permanently and completely erase personal data or de-identify it
- Notify processors to delete personal data

Archive/Backup Systems

- May delay compliance until system is restored to an active system or is next accessed or used

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

23

Universal Opt-Out Mechanism

© 2023 Husch Blackwell LLP

24

Universal Opt-Out Mechanism (UOOM)

- Purpose**
 - Consumers can automatically exercise right to opt out of targeted advertising or sale of personal data through UOOM (but not right to opt-out of profiling)
- Public List of UOOMs**
 - No later than January 1, 2024, the Office will maintain a public list of UOOMs that it has recognized
 - Controllers have 6 months to recognize UOOM added to the list
- Processing of Request**
 - Controller shall treat UOOM as valid opt out request for browser or device and, if known, for the consumer

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

25

Universal Opt-Out Mechanism (UOOM)

- Notice**
 - Controller is permitted, but not required, to display that it has recognized opt-out signals such as by displaying on its website “Opt-Out Preference Signal Honored”
- Consent**
 - Controller may enable consumer to consent to processing for which consumer has opted out so long as request for consent complies with CPA and rules
 - If consumer used UOOM to opt out, then controller cannot interpret later absence of UOOM as consent to opt back in

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

26

UOOMs and Cookie Banners

“A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits the website of a fashion retailer that routinely shares Consumer Personal Data for Targeted Advertising. The fashion retailer must obtain the Consumer’s consent because the Consumer has already opted out of Processing for that purpose. The fashion retailer’s website displays a pop-up banner seeking Consent to share the Consumer’s Personal Data for Targeted Advertising. This is not a valid request for Consumer Consent because the request is made through a pop-up banner that degrades or obstructs the Consumer’s experience on the Controller’s web page or application.”

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

27

UOOMs and Cookie Banners

“A Consumer opts out of the use of Personal Data for Sale or Targeted Advertising using a Universal Opt-Out Mechanism. The Consumer visits a fashion retailer’s website. The fashion retailer’s homepage contains a message at the top of the webpage that displays the Consumer’s opt-out status, stating, “you have opted out of targeted advertising” next to a link that states “Opt-in to Data Use”. The linked webpage also meets all requirements of 4 CCR 904-3, Rules 7.03 and 7.04. Consent pursuant to this request is valid.”

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

28





Privacy Notices

© 2023 Husch Blackwell LLP

29



General Notice Requirements

-  **Understandable** Must be “understandable and accessible to a Controller’s target audiences”
-  **Accessibility** Must comply with Web Content Accessibility Guidelines
-  **Languages** Must be available in languages in which Controller conducts business
-  **Readable** Must be readable on all devices, including on smaller screens and mobile apps

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

30

Privacy Notice Principles

Not Colorado-specific	Controllers do not need to provide a separate Colorado privacy notice or section of privacy notice
Clear	Notice must be clear and avoid abstract or ambivalent terms
Accessible	Must be posted online through conspicuous link using word “privacy” on homepage or app store page or landing page and app settings menu
Specific	Consumers should be able to understand scope of processing

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

31

Privacy Notice

Overview

- A comprehensive description of online and offline processing practices “linked in a way that gives Consumers a meaningful understanding of how each category of their Personal Data will be used when they provide that Personal Data to the Controller for a specified purpose.”

Purpose Specification

- Rule 6.06

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

32

Privacy Notice Contents

Categories of Personal Data Processed

- Including whether personal data of child or other sensitive data is processed
- E.g., “contact information,” “information from cookies”

Processing Purpose

- In level of detail that gives consumers understanding of “how each category of their personal data is used when provided for that” processing purpose

Sell / Targeted Advertising Information

- Whether personal data provided for specific purpose will be sold or used for targeted advertising or profiling
- Categories of personal data sold or shared with third parties
- Categories of third parties to whom controller sells or shares personal data

Profiling Disclosures (if applicable)

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

33



Privacy Notice Contents

✓ List of data rights

📄 Description of methods of submitting requests

👤 Information regarding Sensitive Data Inferences (if applicable)

✉️ Controller’s contact information

🗨️ Instructions on how to appeal

📅 Date privacy notice was last updated

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

34

Changes to Privacy Notice

Notice of Material Changes

- Must notify consumers of “material changes” to privacy notice

Types of Changes

- Includes changes to (1) categories of personal data processed, (2) processing purposes, (3) controller’s identity, (4) act of sharing personal data with third parties, (5) categories of the third parties personal data is shared with, and (6) methods for submitting data rights requests

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

35

Other Data Processing Requirements

© 2023 Husch Blackwell LLP

36

H-B

Purpose Specification



Controllers must specify the “express purpose” for which personal data is collected and processed in both external disclosures to consumers and internal documentation



Must be described in “level of detail that gives Consumers a meaningful understanding of how each category of their Personal Data is used when provided for that Processing purpose”



If data is processed for multiple purposes, controller must specify each

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

37

H-B

Secondary Use

Consent

- Must obtain consumer consent for processing personal data for purposes “not reasonably necessary to or compatible with specified Processing purpose(s)”

Reasonably Necessary or Compatible

- Controllers should consider 7 factors in making determination

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

38

Data Minimization and Retention

Minimization

- Must determine the minimum personal data that is necessary, adequate, or relevant for each express purpose

Retention

- Personal data kept only for as long as necessary for the express purpose
- Shall set specific time limits for erasure or to conduct a periodic review

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

39

Loyalty Programs

© 2023 Husch Blackwell LLP

40

Definitions

“Bona Fide Loyalty Program”

- A “loyalty, rewards, premium feature, discount, or club card program established for the genuine purpose of providing Bona Fide Loyalty Program Benefits to Consumers that voluntarily participate in that program”

“Bona Fide Loyalty Program Benefit”

- An “offer of superior price, rate, level, quality, or selection of goods or services provided to a Consumer through a Bona Fide Loyalty Program”

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

41

H-B

Rules establish structure for:

Interaction between requests to delete / opt out of sale / opt out of targeted advertising and participation in bona fide loyalty program

Consumer refusal to consent to processing of sensitive data necessary for program

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

42



Loyalty Program Disclosures



Categories of personal data or sensitive data collected through program that will be sold or processed for targeted advertising, if any



Categories of third parties that will receive consumer's personal data and sensitive data, including whether personal data will be provided to data brokers



List of program partners and program benefits provided by each program partner



If processing a request to delete makes it impossible to provide program benefit, an explanation of why



If sensitive data is required for program benefit, an explanation of why

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

Sensitive Data

© 2023 Husch Blackwell LLP

Sensitive Data

Consent

- Controllers need consent to process sensitive data and “Sensitive Data Inferences”

Definition of Sensitive Data (§ 6-1-1303(24))

- Personal data **revealing** racial or ethnic origin, religious beliefs, a mental or physical health condition or diagnosis, sex life or sexual orientation, or citizenship or citizenship status;
- Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual; or
- Personal data from a known child.

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

45

Sensitive Data Inferences

“Revealing”

- The word “revealing” in definition of sensitive data includes Sensitive Data Inferences

Definition of Sensitive Data Inferences

- Inferences made by a controller based on personal data, alone or in combination with other data, which are used to indicate an individual’s racial or ethnic origin; religious beliefs; mental or physical health condition or diagnosis; sex life or sexual orientation; or citizenship or citizenship status

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

46

Examples

Precise geolocation data showing individual visited a mosque is sensitive data if used to infer religious beliefs

Precise geolocation data showing individual visited a reproductive health clinic is sensitive data if used to infer health condition or sex life

Web browsing data is sensitive data if used to infer an individual's sexual orientation

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

47

Can process sensitive data inferences *without consent* for individuals over 13 only if:

Obvious

- Processing purpose would be obvious to reasonable consumer

Deletion

- Sensitive data inferences are deleted within 24 hours
- Controller also must disclose information regarding sensitive data inferences in privacy notice and data protection assessment

No Transfer

- Sensitive data inferences are not transferred, sold, or shared

Restricted Processing

- Sensitive data inferences are not processed for any purpose other than disclosed express purpose

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

48

Consent

© 2023 Husch Blackwell LLP

49



5 Requirements for Valid Consent

Obtained through clear, affirmative action

Freely given

Specific

Informed

Reflect consumer's unambiguous agreement

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

50

Clear, affirmative action

Cannot use blanket acceptance of general terms and conditions

Silence is not consent

Inactivity or inaction is not consent

No pre-ticked boxes

Negative option opt-out constructions that require consumer intervention to prevent agreement are insufficient

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

51

Freely given

Cannot use general or broad terms of use with unrelated information

Cannot make performance of contract dependent on processing of personal data unnecessary to contract

Cannot deny goods, services, discounts or promotions if consumer does not consent unless personal data is necessary or as part of loyalty program

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

52

Specific

Consumers must have ability to separately consent to multiple processing purposes that are not reasonably necessary or compatible

Sale of sensitive data to one party is not necessary or compatible with sale of sensitive data to another party

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

53

Informed

Controller's identity

Reason that consent is required

Processing purpose for which consent is sought

Categories of personal data that the controller shall process

Names of all third parties receiving sensitive data through sale (if any)

Description of right to withdraw consent

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

54

Refreshing Consent

24 Months

- If consumer has not interacted with controller in prior 24 months, the controller must refresh consent to process sensitive data and for secondary use purposes if it involves profiling covered by statute's opt out right

Exception

- Controller does not have to refresh consent if consumer has ability to update their opt-out preferences through user-controlled interface

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

55

UI Design, Choice Architecture, and Dark Patterns

© 2023 Husch Blackwell LLP

56

9 Principles

1. Symmetrical Options

- Consent options must be presented in symmetrical way
- Example: “Accept” and “Do Not Accept” buttons in same font, size, and style

2. No Manipulation

- Cannot guilt, shame, or emotionally manipulate
- Example: Using “I want to help endangered species” and “No, I don’t care about animals”

3. Silence Not Sufficient

- Silence or failure to take affirmative action is not consent

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

57

9 Principles

4. No Pre-Selected Consent

- Example: Cannot use pre-selected checkboxes

5. Similar Number of Steps

- Consumer should be able to select either consent choice option with similar number of steps
- Example: Cannot use “I accept” button with “Learn more” button

6. No Interruptions

- Consumer’s interaction on website, app, or product should not be unnecessarily interrupted to request consent

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

58

9 Principles

7. No Misleading

- Cannot use misleading statements, omissions, affirmative misstatements, or intentionally confusing language

8. Consider Vulnerabilities

- Example: Websites directed to individuals under 18 should consider simplicity of language

9. Must Work the Same Through Digital Accessibility Tools

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

59

Data Protection Assessments

© 2023 Husch Blackwell LLP

60

When Required

Heightened Risk

- Required for processing that presents a heightened risk of harm to consumers

Examples

- Targeted advertising
- Sale of personal data
- Processing sensitive data
- Certain types of profiling

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

61

Statutory Requirements

Weigh benefits from processing against potential risks to rights of consumer, as mitigated by safeguards that can be employed by controller to reduce such risks

Use of de-identified data and reasonable expectations of consumer, as well as context of processing and relationship between controller and consumer must be factored into assessment

Only applies to processing activities created or generated after January 1, 2023 (Virginia) or July 1, 2023 (Colorado and Connecticut)

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

62



Colorado Rules

- DPA must be “genuine, thoughtful analysis”
- At a minimum, DPA must describe 13 topics
- Process should include all relevant internal actors and, where appropriate, external parties
- Must complete DPA before initiating processing activity
- Must update DPA periodically (profiling reviewed annually)
- Attorney General can request DPA on 30 days notice

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

63

Scope

- Standard**
 - “Data protection assessments shall be required for activities created or generated after July 1, 2023. This requirement is not retroactive.”
- “Generated”**
 - “A new data Processing activity is generated when existing Processing activities are modified in a way that materially changes the level of risk presented.”
- Material Change**
 - Rules identify 8 factors to consider

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

64

Profiling

© 2023 Husch Blackwell LLP

65



Overview

Right to Opt Out

- Consumer has the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer

“Profiling”

- Any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements

“Decisions that produce legal or similarly significant effects concerning a consumer”

- A decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services.

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

66

Transparency

Notice

- Controllers must provide clear, understandable, and transparent information to consumer in privacy notice

Notice must include (among other things):

- What decision is subject to profiling
- Categories of personal data at issue
- Explanation of logic used
- How profiling is relevant to ultimate decision
- If system has been evaluated for accuracy, fairness, or bias

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

67

Levels of Automated Processing

Solely Automated Processing

- No human review, oversight, involvement, or intervention

Human Reviewed Automated Processing

- Human reviews processing but level of human review does not rise to the level required for Human Involved Automated Processing (e.g., reviewing outputs with no meaningful consideration)

Human Involved Automated Processing

- Human involvement in processing includes “meaningful consideration of available data used in the Processing as well as the authority to change or influence the outcome of the Processing”
- Controller may decide not to take action in response to request but must provide notice to consumer with 7-part explanation

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

68

Data Protection Assessments

Controllers must conduct profiling data protection assessments if profiling presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on consumers
- Financial or physical injury to consumers
- A physical or other intrusion upon the solitude or seclusion, or private affairs or concerns of consumers if the intrusion would be offensive to a reasonable person
- Other substantial injury to consumers

Profiling data protection assessments must:

- Include 12 additional topics
- Be reviewed and updated annually

HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

Subscribe to our blog...

www.bytebacklaw.com



HUSCH BLACKWELL

© 2023 Husch Blackwell LLP

Thank you

David Stauss

david.stauss@huschblackwell.com

© 2023 Husch Blackwell LLP