Before the
Office of the Attorney General
Colorado Department of Law
Denver, CO

Implementation of the Colorado Privacy Act	))	Pre-Rulemaking Considerations

Comments of the Samuelson-Glushko Technology Law and Policy Clinic (TLPC) at Colorado Law

via web submission to coag.gov
May 26, 2022

Richard Koch, Rebecca Lynch, and Stacey Weber • *Student Attorneys*[1]
Contact: Prof. Blake E. Reid, Director
blake.reid@colorado.edu

[1] These comments benefitted from the substantial contributions of Prof. Margot Kaminski.

Executive Summary

The Samuelson-Glushko Technology Law and Policy Clinic (TLPC) at Colorado Law submits these comments in response to the Pre-Rulemaking Considerations for the Colorado Privacy Act ("CPA") released by the Colorado Department of Law (the Department) on April 12, 2022.[2] This comment reflects the views and research of the above-listed TLPC student attorneys.[3] We believe that privacy is integral to safeguarding democracy and that the implementation of the CPA provides a critical opportunity to help vindicate privacy as a fundamental right of all Coloradans. In submitting this comment, we hope to assist the Department in creating a forward-looking model for how technological innovation and privacy can coexist.

This preliminary comment identifies and provides substantive input on three key areas of the CPA:

- Operationalizing processes for consumer notice;
- Best practices for data protection assessments (DPAs); and
- Internal processes for receiving and responding to consumer requests and appeals.

These aspects of the bill represent crucial opportunities to make the CPA more effective.

Where appropriate, we provide examples by scholars and other states and regulatory bodies that have already addressed or begun to address some of these areas. Their work can offer guidance and insight—a menu of options reflecting leading approaches—for the Department of Law. A secondary goal of this comment is to provide the Department with a non-exhaustive but practical encyclopedia of privacy-related resources, which are footnoted throughout and compiled in the appendix.

Notice. First, the Department has the opportunity to clarify what constitutes effective notice for consumers. First and foremost, this implicates the substance and design of disclosures, which touch upon all consumer rights and can shape consumer understanding and choices in relation to those rights. It also implicates

---

[2] *Pre-Rulemaking Considerations for the Colorado Privacy Act*, Colorado Department of Law (Apr. 12, 2022), https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf.

[3] This comment does not represent the views of Colorado Law, the University of Colorado, or any other institutional affiliation.

consent, in the context of sensitive data, and the particular risk of dark patterns to undermine free and meaningful consent by consumers.

Rulemaking should facilitate effective notice, through clear and accessible disclosure, and protect freedom of consent, through capacity for revocation and regulation of dark patterns. Doing so not only will protect consumers and aid their ability to meaningfully make choices in exercising rights, but will also operationalize controller duties such as the duties of transparency and purpose specification.[4]

DPAs. Second, the Department could address best practices for DPAs. A risk-based collaborative government model, combining industry expertise with government enforcement, should aim to stimulate industry engagement and expertise through bottom-up explanations and resist devolution into empty top-down compliance checklists. Ideally, rules could facilitate internal structuring to use DPAs as a tool for ongoing assessment and risk mitigation, as well as documentation for improvement and government supervision.

Similar to effective notice, dynamic use of DPAs not only furthers goals of risk assessment and mitigation, but helps effectuate controller duties. In particular, DPAs go to the heart of the controller duties of data minimization, avoidance of secondary use, and the duty of care.[5]

Consumer Requests and Appeals Processes. Third, rulemaking could consider the role of internal governance to effectuate controller obligations to receive and respond to consumer requests to exercise privacy rights.[6] Obligations to respond to consumer requests pose the opportunity for meaningful consumer empowerment and protection, but risk nullification through industry self-certification, obstruction, or lack of organization and meaningful implementation. Similarly, rulemaking could address minor challenges ancillary to responding to requests, regarding consumer ability to submit requests and exceptions under which controllers may decline to respond to requests.

Rulemaking promoting and guiding internal governance structures could help aid controllers in efficiently meeting compliance obligations to respond to requests. Moreover, the ability of controllers to implement complete responses to consumer requests will significantly determine whether consumers are able to effectively exercise rights under the CPA.

---

[4] *See* C.R.S. § 6-1-1308(1)–(2) (2021).

[5] *Id.* at § 6-1-1308(2), (3), & (5).

[6] *Id.* at § 6-1-1306(1) ("Consumers may exercise the following [rights] by submitting a request . . . [to a controller].").

Other Areas. The CPA contains a number of other important areas that are beyond the scope of our present research and analysis. Nevertheless, we note several areas that similarly deserve careful attention in the rulemaking process, including:

- The application of the CPA to inferences, particularly inferences regarding sensitive information;
- Rules implementing the duties of controllers; and
- The role of automated decision-making processes.

Table of Contents

Discussion

1. Notice

The failure of online privacy protections largely has been the result of intentional technological design decisions, including ineffective notice, misleading "choice architecture,"[7] and deceptive "dark patterns." To summarize the importance of design decisions: "The way [privacy controls] are implemented can significantly affect individuals' choices and their privacy outcomes."[8] That is, how notice is given and how consent streams are intentionally designed by developers can make exercising privacy rights difficult or confusing, and potentially render user choices ineffective. Thus, both the substance of the notice itself—regarding collection and use of data and methods of exercising consumer rights—and the design of that notice (and associated consent streams), can make exercising privacy rights difficult or confusing. In the CPA, only sensitive information is subject to affirmative consent.[9] However, notice plays a significant role beyond consent in informing individuals of the applicability of the available suite of privacy rights regarding personal data and how to exercise them.[10]

This relationship between consumer privacy rights and meaningful notice is reflected in the CPA, beginning with the series of consumer rights at Section 1306(1) that attach to personal data. For a consumer to effectively exercise most of these rights (which include opt-outs, access, and correction), she must receive clear and meaningful notice in a format that she can both understand and act upon. Thus, CPA Section 1308(a) establishes a "Duty of Transparency" that requires data controllers to provide a "reasonably accessible, clear, and meaningful" privacy notice. The Department has the opportunity in rulemaking to clarify what constitutes effective notice, which would both protect consumers and provide clarity for implementing businesses.

Effective notice is the core of the CPA. It is the necessary predicate not only to the exercise of general consumer data rights but also to the consent that is required by

---

[7] Idris Adjerid, Alessandro Acquisti, & George Lowenstein, *Choice Architecture, Framing, and Cascaded Privacy Choices*, Management Science 65(5) 1949-2443 (2019), https://ssrn.com/abstract=2765111.

[8] Hana Habib, Yixin Zou, Adliti Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lori Cranor, Norman Sadeh, & Florian Schaub, *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, USENIX Proceedings of the Fifteenth Symposium on Usable Privacy and Security 387 (2019), https://www.usenix.org/system/files/soups2019-habib.pdf.

[9] C.R.S. § 6-1-1308(4) (2021).

[10] *See* C.R.S. § 6-1-1308(1)(a) (2021).

CPA Section 1308(7) for the processing of sensitive personal data. "Consent" is defined in Section 1301(5) as a "clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement." "Processing" is defined as "the collection, use, sale, storage, disclosure, analysis, deletion, or modification of personal data."

On the face of the statute, the requirement of consent for processing sensitive data logically applies not just to sensitive data a controller themselves collects directly from the consumer, but also to the controller's processing of sensitive personal data gathered from third-party sources or inferred from consumer-provided or third-party provided data.

A goal of effective data privacy law is to ensure that consumer consent is genuinely informed and freely given.[11] The CPA thus requires in Section 1301(5)(c) that consent *may not* be constituted by any "agreement obtained through dark patterns." A dark pattern is defined in Section 1305(9) as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice." The Department thus also has the opportunity to provide rules and guidance on what constitutes true autonomous consent, contrasted with consent obtained through manipulation, deliberate elision, and choice architecture. This requires consideration not just of substance but of design.[12]

As such, standards for notices, including interface design and choice architecture—and their ability to exploit cognitive biases—play a powerful role in privacy notices, choice, exercise of rights, and consent. While the CPA reflects these connections through its attention to privacy notices, consent, and dark patterns, it relies on rulemaking to implement these protections of user notification and autonomy.

---

[11] The EDPB provides guidance regarding consent and transparency. Article 29 Data Protection Working Party, *Guidelines on Consent Under Regulation 2016/679,* EDPB (May 4, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf ("*Guidelines on Consent*"); Article 29 Data Protection Working Party, *Guidelines on Transparency Under Regulation 2016/679*, EDPB (Apr. 11, 2018), https://ec.europa.eu/newsroom/article29/items/622227 ("*Guidelines on Transparency*").

[12] *See generally* Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (2018). Lorrie Cranor has also addressed design. *E.g.*, Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor, *A Design Space for Effective Privacy Notices*, Usenix (Symposium on Usable Privacy and Security, July 2015), https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub. For additional work by Cranor, *see Lorrie Faith Cranor*, Carnegie Mellon Univ., https://www.cmu.edu/epp/people/faculty/lorrie-faith-cranor.html.

Therefore, this section begins by examining privacy notices and addresses best practices for both the substance and form of privacy notices. It then turns to consent and examines how to design consent that is "freely given, specific, informed, and unambiguous" for collection of sensitive data. Finally, it discusses the regulatory dynamics of dark patterns.

1.1. Effective Notice

Notice can be ignored and pro forma, or visible and effective. Our research suggests that effective regulation of notice requires attention both to the substance and the form—including the timing—of disclosures.

The CPA tasks data controllers with a duty of transparency that requires controllers to provide privacy notices that are "reasonably accessible, clear, and meaningful."[13] The CPA's requirement of clarity speaks to the substance of notice, which must be clear to consumers. The CPA's requirement that the notice be meaningful also dictates that the content of the notice must effectively enable exercise of data privacy rights. The CPA's dual requirements of reasonable accessibility and meaningfulness suggest such notice must also be effective by design.

We draw here on a number of sources, including Human-Computer Interaction (HCI) research, the European Data Protection Board Guidelines on transparency under Regulation 2016/679, as last revised on April 11, 2018,[14] FTC guidance,[15] and scholarly research.[16]

1.1.1. Substance

The CPA dictates at a high level what information a data controller must include in a privacy notice.[17] It also requires that such information be clear and meaningful.

---

[13] C.R.S. § 6-1-1308(1) (2021).

[14] *Guidelines on Transparency*, *supra* note 11.

[15] Work by the FTC regarding mobile phone privacy, including discussion of just-in-time notice provides helpful guidance and informed EDPB guidelines in this area. *Mobile Privacy Disclosures: Building Trust Through Transparency*, FTC (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf. For other FTC guidance, *see, Mobile Health App Developers: FTC Best Practices*, Fed. Trade Comm'n (Apr. 2016), https://www.ftc.gov/business-guidance/resources/mobile-health-app-developers-ftc-best-practices.

[16] *E.g.*, *Schaub, Balebako, Durrity, & Cranor*, *supra* note 12.

[17] C.R.S. § 6-1-1308(1)(a) (2021).

The statute does not, however, clarify what "clear" and "meaningful" mean in practice. This subsection provides suggestions drawn from research and regulation, focusing on areas of consensus that suggest a best practice has developed.

The concept of clarity has been extensively addressed by scholars and regulatory bodies such as the Federal Trade Commission and the European Data Protection Board (EDPB). The EDPB has put forth guidelines on what satisfies GDPR requirements to use "clear and plain language"[18] and that notice be "intelligible,"[19] among other best practices for notice.[20] For example, the EDPB offers concrete terms for the requirement to use clear and plain language: that "information should be provided in as simple a manner as possible, *avoiding complex sentence and language structures.*"[21] Similarly, the FTC emphasizes use of plain and direct language.[22]

Numerous commentators have discouraged vague statements in privacy notices. The CPA itself includes a concrete prohibition on vague statements, at least in regards to consent, which rulemaking could clarify applies to privacy notices as well.[23] The EDPB guidelines similarly instruct controllers to provide information in concrete terms rather than relying on abstract terms or "legal qualifiers" such as "may"[24]—even requiring that where indefinite language is used, controllers should

---

[18] *Guidelines on Transparency*, *supra* note 11, at 8–10 (emphasis added).

[19] *Guidelines on Transparency*, *supra* note 11, at 8 (emphasis added).

[20] *E.g., Guidelines on Transparency*, *supra* note 11, at 19–21 (emphasis added) (addressing layered privacy notices and "push" (notices at the point of collection) and "pull" (notices that facilitate engagement such as privacy dashboards) notices).

[21] *Guidelines on Transparency*, *supra* note 11, at 8 (emphasis added).

[22] *Mobile Health App Developers*, *supra* note 15.

[23] *See* C.R.S. § 6-1-1305(a) (2021) ("Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated elements" does not constitute consent.).

[24] *Guidelines on Transparency*, *supra* note 11, at 8–9. The EDPB also lists examples of language that is not sufficiently clear, along with parenthetical explanations of what in the statement is unclear. *Id.* at 9 ("'We may use your personal data to develop new services' (as it is unclear what the "services" are or how the data will help develop them); 'We may use your personal data for research purposes' (as it is unclear what kind of "research" this refers to); and 'We may use your personal data to offer personali[zed] services' (as it is unclear what the "personali[zation]" entails)."). For further discussion on the harms of vague or inscrutable privacy policies and recommendations to remedy them, see *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers*, Fed. Trade Comm'n (Oct. 21, 2021, FTC Staff Report), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-

be able to give account for its use by "demonstrate[ing] *why* the use of such language could not be avoided and *how* it does not undermine the fairness of processing."[25] Similarly, the FTC guidance that entities explain "why" data is collected resonates with the best practice of avoiding ambiguous descriptions.[26] Finally, scholars have explained the negative impact of vague privacy policies upon users and provided suggestions for redress including: the use of standardized terminology across different jurisdictions' regulations; enforcement of a requirement that the provided privacy choices are relevant and accurate; and requirements that controllers clearly describe what choices do—such as identifying the device to which opt-outs apply.[27]

Other best practices and regulations address concrete approaches to keep privacy notices clear, complete, and accessible. For example, the EDPB encourages the use of "bullets and indents to signal hierarchical relationships," indicates a preference for active voice over passive voice, and suggests avoiding excessive nouns and "overly legalistic, technical or specialist language or terminology."[28] California has similarly experimented with requirements setting out specific formatting and subject matter to be addressed.[29]

Regulators and scholars also work to ensure that privacy notices achieve their purpose by attending to the accessibility of the language and format. Thus, EDPB guidance regarding the GDPR requirement of intelligibility is concretely defined as a requirement that information "should be *understood by an average member of the intended audience.*"[30] In fact, it asserts that a controller should specifically use the

---

examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

[25] *Guidelines on Transparency*, *supra* note 11, at 9 (emphasis added).

[26] *Mobile Health App Developers*, *supra* note 12. *See* Lesley Fair, *What Vizio was Doing Behind the TV Screen*, FTC Bus. Blog (Feb. 6, 2017), https://www.ftc.gov/business-guidance/blog/2017/02/what-vizio-was-doing-behind-tv-screen (describing complaint that included allegation that privacy policy's general statements, including that it collected data to "enable[] program offers and suggestions," did not fairly describe granular tracking practices); *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent*, FTC (Feb. 6, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million.

[27] Habib, Zou, Jannu, Sridhar, Swoopes, Acquisti, Cranor, Sadeh, & Schaub, *supra* note 8, at 397.

[28] *Guidelines on Transparency*, *supra* note 11, at 9–10 (emphasis added).

[29] CCPA Regulations, 11 C.C.R. § 305 (2021), https://oag.ca.gov/privacy/ccpa/regs.

[30] *Guidelines on Transparency*, *supra* note 11, at 7 (emphasis added).

knowledge it has about the people whose information it collects—such as the age and education of data subjects—"to *determine what that audience would likely understand*" and, if it is unsure regarding intelligibility, should test the desired language.[31] Others, including California, have adopted regulations to operationalize requirements that the language be plain and easy to understand.[32] Yet the EDPB also notes that the GDPR contains an inherent tension between its extensive notification requirements and any practical ability to meet these in a form that is truly "concise, transparent, intelligible and easily accessible."[33]

On the one hand, regulators want privacy notices to be exhaustive enough to make rights meaningful. On the other, they remain aware that information overload is a problem. Thus, the EDPB and others encourages controllers to take advantage of layering to meet this challenge—providing a "clear overview" of the information provided and where detailed information is unpacked in the notice, such as through section headings, dropdowns, or a hyperlinked table of contents—but suggesting care when doing so to avoid providing conflicting information across layers.[34] Other strategies to avoid information fatigue[35] noted by the EDPB include presenting information succinctly and differentiating privacy-related information from non-privacy-related information, such as terms of use.[36]

Finally, the Department could consider a requirement, similar to EDPB guidance, reminding controllers to be attentive to the ongoing accuracy and applicability of privacy policies. Such a requirement would ensure that stated policies accurately

---

[31] *Guidelines on Transparency*, *supra* note 11, at 7 (emphasis added).

[32] CCPA Regulations, 11 C.C.R § 999.305 (2021). Notably, the CPA also attends to the importance of easy consumer understanding and of various rights, information, and resources. C.R.S. § 6-1-1302(1)(c), 1306(1)(a)(IV)(C), 1306(3)(a), 1308(1)(a), 1313(1)(d) (2021).

[33] *Guidelines on Transparency*, *supra* note 11, at 18 (emphasis added).

[34] *Guidelines on Transparency*, *supra* note 11, at 7, 19 (emphasis added). The EDPB even sets out priority of what information should be included in which layer—for example, the first layer should include a description of privacy rights and processing that could surprise the data subject, among other suggested pieces of information—and suggests controllers pair layering in notices with other mechanisms such as specific notice at the point of collection. *Id.* at 19; *see also* Schaub, Balebako, Durity, and Cranor, *supra* note 12; Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper, *Harder to Ignore? Revisiting Pop-up Fatigue and Approaches to Prevent It*, Symposium on Usable Privacy and Security (July 2014), https://www.usenix.org/conference/soups2014/proceedings/presentation/bravo-lillo.

[35] *Guidelines on Transparency*, *supra* note 11, at 6–7 (emphasis added).

[36] *Guidelines on Transparency, supra note* 11, at 7 (emphasis added).

reflect use across the collection and processing lifecycle, and that policies are updated—and relevant updates communicated to users[37]—when collection and processing practices significantly change.[38]

1.1.2. Form and Design

The CPA addresses the design of effective notice by requiring that data controllers implement notice that is "reasonably accessible" and "meaningful."[39] This subsection first discusses what it means for notice to be reasonably accessible, then turn to how notice can be designed to be meaningful—or not.

The CPA's reasonably accessible requirement resonates strongly with the GDPR's "easily accessible" requirement.[40] Thus, rulemaking could be informed by other sources of guidance addressing designs that do—or do not—facilitate accessibility.

For example, the FTC has warned against making hyperlinks difficult to locate.[41] The EDPB similarly explains that a user "should not have to seek out the information; it *should be immediately apparent* to them where and how this information can be accessed, for example by providing it directly to them, by *linking* them to it, by *clearly signposting* it or as an *answer to a natural language question.*"[42]

Commentators have also discussed various strategies to facilitate accessibility of notices. These include use of a variety of navigable mechanisms such as layering, contextual pop-ups, and interactive assistance such as a chatbot—while noting that

---

[37] *See Guidelines on Transparency*, *supra* note **11**, at 17 ("Changes to a privacy statement/notice that should always be communicated to data subjects include. . . : a change in processing purpose; a change to the identity of the controller, or a change as to how data subjects can exercise their rights in relation to the processing.").

[38] *Guidelines on Transparency*, *supra* note **11**, at 16. The EDPB also identifies factors to aid controllers in identifying material changes, focusing on the experience of data subjects: "the impact on data subjects (including their ability to exercise their rights), and how unexpected/ surprising the change would be to data subjects." *Id.* at 16–17. *See Mobile Health App Developers*, *supra* note **15**. Both bodies also recommend use of icons or lights to attract user attention.

[39] C.R.S. § 6-1-1308(1)(a) (2021).

[40] *Guidelines on Transparency*, *supra* note 11, at 7–8 (emphasis added).

[41] *Mobile Health App Developers*, *supra* note 15. Similarly, the EDBP warns against placement and color/format schemes that make information less noticeable. *Guidelines on Transparency*, *supra* note 11, at 8.

[42] *Guidelines on Transparency*, *supra* note 11, at 8 (emphasis added).

overuse even of innovative ideas can still cause information fatigue and undermine utility. [43]

The Department should consider these conversations, and the benefit that a variety of notice mechanisms inherently provides to gain and maintain attention of users. Thus, it might note several available and compliant means of notice, possibly including both notices at the point of collection ("just-in-time," or "push" notices), as well as independently accessible and navigable notices ("pull notices" such as privacy dashboards).[44]

Accessibility also goes beyond aesthetic design to include functional aspects of design—i.e., how difficult it is to locate information or exercise a choice, and the timing of that choice. A heuristic suggested by the EDPB—particularly suitable for apps but also applicable to websites—is to ensure that "information is *never more than 'two taps away*.'"[45] Other strategies address the timing and extent of choice, such as suggesting links to privacy policies when notice is given at the point of collection,[46] and even specific techniques such as visceral notice.[47] A common goal

---

[43] *Compare Guidelines on Transparency*, *supra* note 11, at 8 (emphasis added) *and Mobile Health App Developers*, *supra* note 15 (discussing various mechanisms for notice), *with* Bravo-Lillo et al., *supra* note 34 (noting pop-up fatigue) and Cranor et al, *supra* note 8, at 397–98 (noting that lack of unified or consistent location on websites where consumers can seek to exercise opt-out rights leads to confusion and undermines user ability to exercise rights, and suggesting both use of links and centralization of links to address this confusion).

[44] *See Guidelines on Transparency*, *supra* note 11, at 20–21. ("A just-in-time notice is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/notice containing information that is difficult to understand out of context.").

[45] *Guidelines on Transparency*, *supra* note 11, at 8 (emphasis added). This is also reflected in the Dark Patterns discussion below, where a consistent example of dark patterns includes architecture requiring additional effort to withhold information. See discussion *infra* Section 1.3.

[46] *Guidelines on Transparency*, *supra* note 11, at 8; *see also Mobile Health App Developers*, *supra* note 15 (recommending both privacy policies and notice at the point of collection).

[47] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1027 (2013), http://scholarship.law.nd.edu/ndlr/vol87/iss3/3 ("Unlike traditional notice that relies upon text or symbols to convey information, emerging strategies of 'visceral' notice leverage a consumer's very experience of a product or service to warn or inform. A regulation might require that a cell phone camera make a shutter

of these approaches is to furnish the user with the relevant information that imparts sufficient understanding, without requiring him to hunt for it.

Overall, different bodies take different approaches regarding the presentation of a privacy notice. For example, the overarching approach of the California Privacy Protection Agency (CPPA) in implementing California legislation is more prescriptive.[48] Comments by the Colorado Attorney General, on the other hand, appear to favor a more principled and flexible approach.[49] In the middle, the Connecticut Data Privacy Act has a similar structure and principled approach as the Colorado Act, but includes greater detail in some provisions in the act itself instead of providing Attorney General Rulemaking.[50]

The Attorney General's remarks suggest that EDPB guidance and identification of threshold qualifiers of those principles may aid articulating and enforcing those guiding principles. While the GDPR does not prescribe the format or modality by which such information should be provided to the data subject, it does make clear that the data controller bears affirmative responsibility to take "appropriate measures" given the circumstances of collection and processing in relation to the

---

sound so people know their photo is being taken.") (citations omitted); *see also* Calo at 1035 ("You can write a lengthy privacy policy that few will read, *or* you can design the website in a way that places the user on guard at the moment of collection or demonstrates to the consumer how their data is actually being used in practice."). Arguably, EDPB guidance reflects this practical attitude in focusing on the experience of the user as the lodestar of compliance.

[48] *See, e.g.,* Cal. Civ. Code 1.18.5 § 1798.185 (2021) (listing areas for CPPA rulemaking); Malia Rogers, *CPRA Update: California Privacy Protection Agency Announces Rulemaking Timeline*, Byte Back (Feb. 17, 2022), https://www.bytebacklaw.com/2022/02/cpra-update-california-privacy-protection-agency-announces-rulemaking-timeline (noting that the CPPA now expects to complete rulemaking by the end of 2022 rather than in July, as originally required in the legislation).

[49] *A Conversation with Colorado Attorney General Phil Weiser*, Data Privacy Unlocked: Legislating Data Privacy Series (May 9, 2022), available via major podcast platforms or at https://www.bytebacklaw.com/2022/05/legislating-data-privacy-series-a-conversation-with-colorado-attorney-general-phil-weiser.

[50] An Act Concerning Personal Data Privacy and Online Monitoring, Pub. Act No. 22-15 (2022), https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022. For a comparison of the Connecticut Bill to other state privacy bills passed to date, see *Webinar: Analyzing the Connecticut Data Privacy Act*, Byte Back (May 2, 2022), https://www.bytebacklaw.com/2022/05/webinar-analyzing-the-connecticut-data-privacy-act.

provision of the required information for transparency purposes.[51] It also offers guidance to determine those appropriate measures, such as conducting trials and soliciting feedback on various modalities before a chosen notice is adopted, and documenting the adoption process.[52]

1.2. Consent

Section 1308(7) of the CPA requires consent for the processing of sensitive data. It defines consent as "a clear, affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement."[53] The CPA exempts from its definition of consent "(a) acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information, (b) hovering over, muting, pausing or closing a given piece of content, and (c) agreement obtained through dark patterns."[54] In this subsection we discuss how to design consent that is "freely given, specific, informed, and unambiguous."

The design of consent streams or choice architecture can either enable or prevent effective consent. For example, one Facebook consent flow in recent years required three clicks to provide consent for data collection, including facial recognition, but fourteen clicks to decline.[55] Further, the standard and enforcement of consent has significant consequences; Amazon recently won partial dismissal for a suit claiming Wiretap Act and other illegal interceptions by collecting recordings of communication to Alexa, on the basis that registered users, at least, provided consent by agreeing to the Conditions of Use upon registration of the device.[56]

---

[51] *Guidelines on Transparency*, *supra* note 11, at 14.

[52] *Guidelines on Transparency*, *supra* note 11, at 14. Such documentation also aids in Data Protection Assessments. *See* discussion *infra*, Part 2.

[53] C.R.S. § 6-1-1303(5) (2021).

[54] *Id.*

[55] Arunesh Mathur, *Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites*, slide 9 (2019), http://aruneshmathur.co.in/files/talks/CSCW19_DarkPatterns_Slides.pdf. The associated paper won a 2021 FPF Privacy Papers for Policymakers award, *see infra* note 80. A more recent paper, Arunesh Mathur, Jonathan Mayer, & Mihir Kshirsagar, *What Makes a Dark Pattern…Dark? Design Attributes, Normative Considerations, and Measurement Methods* (Jan. 13, 2021), https://arxiv.org/abs/2101.04843, was spotlighted at the recent FTC workshop on Dark Patterns, *see infra* note 81.

[56] Jake Holland, *Amazon Alexa Suit's Registered User Wiretap Claims Axed*, Bloomberg Law (May 9, 2022), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X72JHUV8000000?bna_news_filter=privacy-and-data-security#jcite.

Similar to the CPA, the GDPR breaks down "valid consent" into multiple constituent elements, requiring it to be: (1) freely given, (2) specific, (3) informed, and (4) unambiguous/affirmative."[57] As such, its guidance on these terms and the related work of scholars offer a framework for how Colorado could—and how industry likely already does—understand these terms.

First, the CPA requires that consent be freely given.[58] EDPB guidelines on this element adopts a presumption that consent "bundled" with non-negotiable terms and conditions is not freely given.[59] This anti-bundling concept would lead to different results in scenarios such as the Amazon Alexa episode noted above, and could enable state privacy laws to protect and empower consumers where other federal and state laws currently do not. It would also build on recent development in the FTC enforcement position regarding negative option marketing, as seen in its recent assertion that consent for auto-enrollment in a subscription must be given separately from other terms and conditions.[60]

Proliferation or inconsistency of consent interfaces can cause confusion as consumers attempt to exercise consent on various sites or platforms. Thus, practical measures to "unify multiple choice mechanisms into a single interface, or provide one single mechanism for a particular type of privacy choice"[61] could provide a helpful counterbalance.

Researchers recommend simplifying processes so that consent cannot become a new battleground for manipulation.[62] This is discussed in-depth *infra* in the context of dark patterns, but it is also relevant to consider as an aspect of beneficial choice architecture and transparent interface design. For example, simple requirements that simplify the exercise of privacy choices, or automatically save them, as well as

---

[57] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) ("GDPR").

[58] C.R.S. § 6-1-1303(5) (2021).

[59] *Guidelines on Consent*, *supra* note 11 at 7.

[60] FTC, *Enforcement Policy Statement Regarding Negative Option Marketing*, FTC 13 (Nov. 4, 2021), https://www.federalregister.gov/documents/2021/11/04/2021-24094/enforcement-policy-statement-regarding-negative-option-marketing ("*Negative Option Marketing Enforcement Policy Statement*"). Notably, this emphasis on separation to empower consent is reflected in the CPA definition of consent at C.R.S. §6-1-1303(5)(a).

[61] Habib, Zou, Jannu, Sridhar, Swoopes, Acquisti, Cranor, Sadeh, & Schaub, *supra* note 8, at 397–98.

[62] *See* Dark Patterns discussion *infra* Section 1.3.

enforcement that identifies bad actors that impose burdens, could all inform rules that establish the characteristics of well-designed choice and consent.[63]

The EDPB considers the ease of revocation as an aspect of whether consent is freely given, and considers consent not free if consent cannot be refused or withdrawn "without detriment."[64] This issue was also recently taken up by the French data protection authority, CNIL, in the context of cookies, which proposes that it must be as easy to withdraw consent as it is to give it.[65]

Ease of revocation remains an area where the CPA needs clarification through rulemaking. Currently, it explicitly requires revocation as easy as consent to override a universal opt-out.[66] However, this standard is not explicitly applied to revocation of consent to process sensitive data. However, both the elements of consent and the prohibition on dark patterns, discussed *infra*,[67] provide ground for the Department to clarify this protection in all circumstances requiring consent in the CPA.

In addition to ease of revocation, the Department could note other indicators of manipulated consent, such as conditionality and exploitation of a power imbalance. Again, the EDPB has already identified these as factors that inform whether consent is freely given. Conditionality reflects specific situations "of tying consent into contracts or the provision of a service," while attention to power imbalance generally reflects "the notion of imbalance between the controller and data

---

[63] Habib, Zou, Jannu, Sridhar, Swoopes, Acquisti, Cranor, Sadeh, & Schaub, *supra* note 8, at 397–98.

[64] *Guidelines on Consent*, *supra* note 11, at 5. As reflected in the CPA regarding consent to override a universal opt-out, consent must be able to be revoked as easily as it is given in order to be considered freely given. *GDPR: Consent*, GDPR-Info, https://gdpr-info.eu/issues/consent.

[65] CNIL, *Cookies Equally Easily Accepted or Refused: the CNIL Sends a Second Series of Orders to Comply* (July 23, 2021), https://www.cnil.fr/en/cookies-equally-easily-accepted-or-refused-cnil-sends-second-series-orders-comply; *see also CNIL's New Guidelines and Recommendations on Cookie Consent*, CookieYes (July 14, 2021), https://www.cookieyes.com/blog/cnil-guidelines-and-recommendations-on-cookie-consent.

[66] C.R.S. § 6-1-1306(1)(a)(IV)(C) (2021); *see also* GDPR*: Consent,* GDPR-Info, https://gdpr-info.eu/issues/consent (last accessed May 16, 2022),(explaining that the ease of revocation requirement exists to implement the GDPR's requirement that consent be revoked as easily as it is given).

[67] *See* discussion *infra*, Section 1.3.

subject."[68] In addition to facilitating consistency across regulatory regimes, attention to these principles to guide protection of consent is resonant with controller duties under the CPA to avoid secondary use and to promote data minimization.[69]

Next, regarding the requirement that consent must be specific, the EDPB sets out three elements. These are that "the controller must apply:

i. Purpose specification as a safeguard against function creep,

ii. Granularity in consent requests, and

iii. Clear separation of information related to obtaining consent for data processing activities from information about other matters."[70]

Again, this framework not only aligns understanding of the terms used in the CPA that already have some familiarity for entities regulated by the GDPR, but also resonates with CPA duty of purpose specification[71] and the duty to avoid secondary use.[72]

The EDPB also considers the CPA elements of consent that require an "affirmative act signifying . . . unambiguous agreement"[73] as closely related, framing an affirmative act as the indicator for unambiguous consent.[74] As such, the EDPB explicitly concludes that "the use of pre-ticked opt-in boxes is invalid under the GDPR,"[75] as is "[s]ilence or inactivity on the part of the data subject." [76] When

---

[68] *Guidelines on Consent*, *supra* note 11, at 7–11. The EDPB also adopts a presumption that "consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service." *Id.* at 10. This is at least resonant with the CPA duties to avoid secondary use and minimization.

[69] C.R.S. § 6-1-1308(3)–(4) (2021).

[70] *Guidelines on Consent*, *supra* note 11, at 14.

[71] C.R.S. § 6-1-1308(2) (2021).

[72] *See* C.R.S. § 6-1-1308(4) (2021).

[73] C.R.S. § 6-1-1303(5) (2021).

[74] *Guidelines on Consent*, *supra* note 11, at 18 (noting unambiguous indication "must always be given through an active motion or declaration").

[75] *Guidelines on Consent*, *supra* note 11, at 18.

[76] *Guidelines on Consent*, *supra* note 11, at 18*; see also* Press Release, *FTC to Ramp Up Enforcement Against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions*, FTC (Oct. 28, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions. As

addressing the balance of how disruptive a request for consent should be, the EDPB opts for interruption of the user experience when necessary to avoid ambiguity in giving consent, but maintains that "the request for consent should not be unnecessarily disruptive."[77] Again, this approach resonates with recent FTC guidance limiting auto-consent[78] and the opportunity for the Department to establish broader protection for consumers' sensitive information.

1.3. Dark Patterns

The CPA defines consent so as to exclude "consent obtained through dark patterns" at Section 1303(5)(c). The CPA defines "dark patterns" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice."[79]

Some researchers similarly define dark patterns as "user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make."[80] While there is no globally standardized regulatory definition for "dark patterns," "[e]verybody has seen them before and found them frustrating."[81]

Dark patterns in this context can be characterized as a particularly nefarious and deliberate version of choice architecture whereby users are deceived into "choosing" something they affirmatively did not want or would not have chosen under a neutral configuration. Dark pattern designers "rely heavily upon interface

---

discussed *infra* Part 1.3.2, FTC enforcement has begun to frame automatic consent in negative option marketing as an illegal dark pattern.

[77] *Guidelines on Consent*, *supra* note 11, at 19.

[78] *Negative Option Marketing Enforcement Policy Statement*, *supra* note 60, at 13–14.

[79] C.R.S. § 6-1-1303(9) (2021).

[80] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. 3, CSCW 81, 2 (2019), https://doi.org/10.1145/3359183.

[81] Lior Strahilevitz and Jamie Luguri, *Shining a Light on Dark Patterns*, 13 U of Chic. J. of L. Analysis, Pub. L. Working Paper No. 719 44 (2021), https://academic.oup.com/jla/article/13/1/43/6180579. This paper is spotlighted on the California Attorney General webpage, https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/shining-a-light-on-dark-patterns.pdf, and its authors presented as panelists during the recent FTC workshop and associated comments on dark patterns, *Bringing Dark Patterns to Light*, FTC (Apr. 29, 2021), https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop.

manipulation, such as changing the hierarchy of interface elements or prioritizing certain options over others using different colors."[82]

There is striking empirical support for the proposition "that dark patterns are effective in bending consumers' will."[83] They are also most effective—and lucrative—when subtly employed,[84] making the task of differentiating dark patterns from permissible marketing or aesthetics challenging. Finally, dark patterns have a disproportionate adverse impact on people with less education, raising equity concerns.[85]

To enforce the CPA's prohibition on use of dark patterns to obtain consent the Department might consider taking a two-pronged approach: both identifying a general test as to when a dark pattern has been used to obtain consent, and providing clarity of that general test by offering a taxonomy of features typical to dark patterns and, over time, identifying specific instances of dark patterns.

In the following subsection we identify two possible tests, proposed by researchers, for determining when a dark pattern has been used: a multi-factor intent-based test and a performance-based test.

1.3.1. Tests for Identifying Dark Patterns

Lior Strahilevitz proposes an intent-based multi-factor test in which regulators consider:

> (i) evidence of a defendant's malicious intent or knowledge of detrimental aspects of the user interface's design,
>
> (ii) whether vulnerable populations—like less educated consumers, the elderly, or people suffering from chronic medical conditions—are particularly susceptible to the dark pattern, and
>
> (iii) the magnitude of the costs and benefits produced by the dark pattern . . . ."[86]

While appealing, this test has limitations. For one, it could be difficult to prove companies' intent and a search for intent might unnecessarily drain Department

---

[82] Mathur, Acar, Friedman, Lucherini, Mayer, Chetty, & Narayanan, *supra* note 80 at 7.

[83] Strahilivetz & Luguri, supra note 81 at 64.

[84] *Id.* at 46–47.

[85] *Id.* at 80.

[86] Stahillevitz & Luguri, *supra* note 81 at 99.

resources. Similarly, a focus on intent may not capture dark patterns arising from carelessness in website design. Additionally, a multi-factor test might not provide enough clarity either for regulators or for regulated entities, falling short of the value of guidance to aid stability and some amount of certainty. Finally, a multi-factor test that requires cost-benefit analysis leaves room for companies to work around the definition through new practices[87] and at the same time might not allow sufficient flexibility.

A second approach is performance-based regulation. Performance-based regulation "sets a measurable standard closer to the regulator's ultimate goal and allows the regulated entity to choose how to meet that standard."[88]

In application, the performance-based approach would seek to "recommend performance-based standards for identifying dark patterns, measuring their impact, and posit methods for evaluating them."[89] The text of the CPA lends itself to this approach in its focus on patterns that have "the substantial effect of subverting or impairing user autonomy."

A benefit of a performance-based approach is that it "shifts the burden of proof from individual consumers to large firms, while still providing enough flexibility for companies to determine how to best meet performance goals."[90] Paired with guidance, it could avoid outcome-based rules that are "too narrow to identify gray areas" or worse, "spur a race among designers to exploit loopholes in interpreting definitions or measurement of outcomes."[91]

1.3.2. Taxonomy of Features and Specific Instances of Dark Patterns

Once the Department selects a general test for identifying dark patterns, the Department might consider (a) outlining a taxonomy of particular features that often, though not always, indicate a dark pattern; (b) enumerating certain specific practices as dark patterns in an open list, whether in regulation or in guidance; and (c) releasing guidance that identifies particular instances of dark patterns on an ongoing basis.

---

[87] Jennifer King & Adriana Stephan*, Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from California Privacy Rights Act*, 5 Geo. L. Tech. Rev. 251, 263 (2021), https://georgetownlawtechreview.org/wp-content/uploads/2021/09/King-Stephan-Dark-Patterns-5-GEO.-TECH.-REV.-251-2021.pdf.

[88] *Id.*

[89] *Id.* at 275.

[90] *Id.* at 263.

[91] *Id.* at 274.

One set of researchers evaluating dark patterns at scale determined that dark patterns often share one or more of five generalized features, which the study terms "dimensions." This taxonomy of features could be useful both for the Department in determining when a dark pattern is at play, and for regulated companies evaluating whether their practices constitute a dark pattern.[92]

In particular, these researchers found that dark patterns often include in consent streams:

1. *Asymmetric* designs that "impose unequal weights or burdens on the available choices presented to the user in the interface;"[93]
2. *Covert* designs that hide the effects of design choices from users;[94]
3. *Deceptive* designs that "induce false beliefs either through affirmative misstatements, misleading statements, or omissions."[95]
4. *Restrictive* designs that "restrict the options available to users so as to force particular choices;"[96] and/or,
5. Designs that *hide* information by "obscur[ing] or delay[ing] the presentation of necessary information to the user."[97]

European regulators also offer valuable insight on identifying and enforcing against dark patterns. CNIL has released expansive guidance that addresses both dark patterns and larger questions around interface design and choice architecture

---

[92] Mathur, Acar, Friedman, Lucherini, Mayer, Chetty, & Narayanan, *supra* note 80 at 5.

[93] *Id.* at 6 ("For instance, a website may present a prominent button to accept cookies on the web but make the opt-out button less visible, or even hide it in another page.").

[94] *Id.* at 6 ("For instance, a website may leverage the decoy effect cognitive bias, in which an additional choice—the decoy—is introduced to make certain other choices seem more appealing. Users may fail to recognize the decoy's presence is merely to influence their decision making, making its effect covert.").

[95] *Id.* at 6 ("For instance, a website may offer a discount to users that appears to be limited-time, but actually repeats when the user refreshes the website's page. Users may be aware that the website is trying to offer them a discount; however, they may not realize that they do not have a limited time to take advantage of the deal. This false belief affects users' decision-making i.e., they may act differently if they knew that the sale is recurring.").

[96] *Id.* at 7 ("For instance, a website may only allow users to sign up for an account with existing social media accounts so they can gather more information about them."

[97] *Id.* at 7 "For instance, a website may not disclose additional charges for a product to the user until the very end of their checkout.").

similar to the discussion above,[98] as well as paved the way for what enforcement of violations could look like.[99]The European Data Protection Board (EBPB) recently released guidelines on dark patterns that offer a taxonomy of dark pattern features.[100] The EDPB identifies six features common to dark patterns: Overloading,[101] Skipping,[102] Stirring,[103] Hindering,[104] Fickle,[105] and Left in the Dark.[106]

The Department might draw on features across these resources in developing a taxonomy of features of dark patterns for its regulations, guidance, and enforcement. There is some substantive overlap between the approaches, particularly reflecting a focus on insufficient or ineffective disclosure, omission of

---

[98] *Shaping Choices in the Digital World*, CNIL (Jan. 2019), https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[99] *CNIL Fines Google €50 Million for Alleged GDPR Violations*, Hunton Privacy Blog (Jan. 23, 2019), https://www.huntonprivacyblog.com/2019/01/23/cnil-fines-google-e50-million-for-alleged-gdpr-violations (ruling based on burden to mobile phone users who need "up to five or six actions to obtain the relevant information about the data processing" when creating a Google account).

[100] *Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognize and avoid them,* EDPB (Adopted on Mar. 14, 2022), https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf ("Guidelines on Dark Patterns").

[101] *Id.* ("users are confronted with an avalanche/ large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of data subject.").

[102] *Id.* ("designing the interface or user experience in a way that the users forget or do not think about all or some of the data protection aspects").

[103] *Id.* ("affects the choice users would make by appealing to their emotions or using visual nudges.").

[104] *Id.* ("an obstruction or blocking of users in their process of getting informed or managing their data by making the action hard or impossible to achieve").

[105] *Id.* ("the design of the interface is inconsistent and not clear, making it hard for users to navigate the different data protection control tools and to understand the purpose of the processing.").

[106] *Id.* ("an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights").

information, and particular ways in which interface design constrains and channels user behavior.

2. Data Protection Assessments

CPA Section 1309(1) requires controllers to "conduct and document a data protection assessment of each of its processing activities that involve personal data" in circumstances presenting a heightened risk of harm. Such processing includes but is not limited to: processing sensitive data; selling data; and processing personal data for the purposes of targeted advertising or profiling that causes a substantial injury to consumers, among other kinds of injuries.[107]

Under CPA Section 1309(3), all such assessments ("DPAs") are required to "identify and weigh the benefits that may flow, directly and indirectly, from the processor to the controller, the consumer, others stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing." DPAs must also include how such risks can be mitigated by the use of safeguards, factoring in: (1) "the use of de-identified data," (2) "the reasonable expectations of consumers," (3) "the context of the processing," and (4) "the relationship between the controller and the consumer."

There is increasing policy consensus over the central importance of DPAs. Data protection impact assessments ("DPIA") are required under the GDPR for high-risk processing.[108] The California Privacy Rights Act (CPRA) amended the CCPA to require businesses whose data processing presents significant risks to privacy or security to conduct risk assessments to be submitted to the California Privacy Protection Agency (CPPA).[109] Similarly, the FTC has used regular impact assessments and risk mitigation as a settlement requirement in instances of privacy violations.[110]

At its worst, a DPA is an empty compliance checklist.[111] But at its best, a DPA acts as an ongoing risk mitigation process that lowers the potential for real harm to consumers. "The procedures an impact assessment puts in place can serve not just

---

[107] C.R.S. § 6-1-1309(2) (2021).

[108] GDPR Art. 35

[109] Cal. Civ. Code til. 1.81.5, California Consumer Privacy Act of 2018 (2022), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[110] *E.g.*, Order Modifying Prior Decision and Order, In the Matter of Facebook, Inc., VII.D–E, FTC Docket No. C-4365 (Apr. 27, 2020), https://www.ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf.

[111] *See generally* Ari Waldman, *Privacy, Practice, and Performance,* 110 Cal. L. R. 1 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784667.

to prevent error, bias, and discrimination, but also to legitimize a system or even respect an individual's dignity within it."[112]

Rulemaking that emphasizes that the DPA is an ongoing process can protect the DPA requirement from devolving into an empty compliance checklist. The Department could identify the substantive values at stake and minimum standards or guiding principles for compliance, coupled with selective review and enforcement of compliance with controllers' duties and promised risk mitigation (such as A/B dark pattern auditing). Similarly, the Department could institute processes for entities to receive feedback from consumers and impacted stakeholders. Finally, the DPA process not only can establish procedures for complying with controller duties under the CPA, but information gathered by a company during a data protection assessment can in turn be used as the basis for required disclosures to consumers.[113]

As such, we encourage the Department to consider existing models for DPAs, specific components that should be included in a DPA, and methods for effectively enforcing the DPA requirements.

2.1. DPA Models

At the highest level, a DPA regulation has two main goals

1. To require firms to consider social impacts early and work to mitigate risks before and during deployment; and
2. To create documentation of decisions and testing that can support both government enforcement and future policy-learning.[114]

For impact assessments to serve as effective risk management, they need to be not just static documents but ongoing processes.[115] Controllers should build in risk

---

[112] Margot Kaminski & Gianclaudio Malgieri, *Algorithmic impact assessments under the GDPR: producing multi-layered explanations*, 2 Int. Data Privacy L. 11 125, 138 (2021), https://academic.oup.com/idpl/article /11/2/125/6024963.

[113] *Id.*

[114] Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 Harv. L. J. & Tech. 117, 118 (2021), https://jolt.law.harvard.edu/assets/articlePDFs/v35/Selbst-An-Institutional-View-of-Algorithmic-Impact-Assessments.pdf.

[115] The EDPB has adopted working group guidance. Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679*, WP248 (Oct. 13, 2017), https://ec.europa.eu/newsroom/article29/items/611236/en ("*DPIA Guidelines*"); *see also* Kaminski & Malgieri, *supra* note 112; *Risk Management*, NIST,

mitigation at the onset. In fact, early intervention is crucial because regulators "need to know how many of the subjective decisions that go into building a model led to the observed results, and why those decisions were thought justified at the time."[116] But assessments should also be ongoing: controllers should monitor the use of a system for actual harms and constantly update their risk mitigation approach accordingly.[117] DPAs "should thus be truly continuous: a process that produces outputs or reports, but also includes ongoing assessment and performance evaluation, especially for those [design processes] that change quickly over time and are deployed in multiple contexts."[118]

The CPA states that a controller "shall not conduct processing that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment."[119] The Department could interpret this provision, with its gerunds of "conduct*ing*" and "document*ing*," to involve not just a static document produced before processing, but an ongoing documented risk mitigation process, similar to the GDPR's Data Protection Impact Assessment.

Beyond this initial question of whether an assessment is a document or a process, contemporary data protection impact assessments (or algorithmic impact assessments) tend to take one of three forms:

1. Internal enterprise risk management, with no oversight by regulators or release to the public;
2. Risk-based governance delegated to a private party but overseen by the government ,also known as "collaborative governance"; or
3. Risk mitigation through public policymaking.[120]

The first model, enterprise risk management, relies on companies to self-govern by voluntarily assessing and mitigating risks associated with data processing. NIST's Cybersecurity Risk Management Framework is a well-established version of this approach;[121] NIST's more recent draft AI Risk Management Framework is another

---

https://www.nist.gov/risk-management (providing several NIST frameworks for cybersecurity, risk management, and privacy) (last accessed May 17,. 2022).

[116] Selbst, *supra* note 114 at 147.

[117] *See DPIA Guidelines, supra* note 115 at 14.

[118] Selbst, *supra* note 114 at 140.

[119] C.R.S. § 6-1-1309(1) (2021).

[120] Margot Kaminski, *Regulating the Risks of AI,* BU Law Review (forthcoming 2023) (draft on file with authors).

[121] *Cybersecurity Framework,* NIST https://www.nist.gov/cyberframework (last accessed May 17, 2022).

example.[122] In this model, both the public and the government play no official role and are largely uninvolved.

By contrast, the second model, risk-based collaborative governance, uses the impact assessment process to spur companies to use their expert knowledge, resources, and organizational infrastructure to "co-govern" themselves and reduce risks, under threat of possible government enforcement.[123] Under this model, the impact assessment serves not just as voluntary risk mitigation, but also as a way of establishing governance procedures within companies, and to document choices that regulators may later examine or enforce.

The GDPR's Data Protection Impact Assessment is an example of this approach, as are the conformity assessments proposed in the draft EU AI Act. The official guidance on the GDPR's DPIAs recommends making a summary of the DPIA public, but formal publication is not explicitly required.[124]

While not always involving mandatory public disclosure of impact assessments, this second model still characterizes the assessments as proto-policymaking. That is, under the collaborative governance model, regulators may use their insights gleaned from their oversight and enforcement of impact assessments to later put in place concrete and enforceable rules and standards for an entire industry.

The third model views impact assessments as a crucial tool of public policymaking. Modeled after the Environmental Impact Statement required under the National Environmental Policy Act ("NEPA"), this model centrally entails releasing assessments for public notice and comment. [125] A proposed Washington state law, SB 5116, similarly would require the release of public sector algorithmic accountability reports for public comment.[126] Under this model, impact assessments not only mitigate risk but inform and involve the public of the potential harms of a

---

[122] *AI Risk Management Framework,* NIST https://www.nist.gov/itl/ai-risk-management-framework (last accessed May 17, 2022).

[123] *See generally* Margot Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529 (2019), https://scholar.law.colorado.edu/articles/1265; Kaminski & Malgieri, *supra* note 112.

[124] *DPIA Guidelines*, *supra* note 115 at 18; *see also,* GDPR, *supra* note 57, , art. 35, recitals 84, 90–93,,.

[125] Selbst, *supra* note 114 at 141.

[126] *See* Wash. S. Rep. No. 5166 (2021), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bill%20Reports/Senate/5116%20SBR%20SGE%20TA%2021.pdf ("State and local government agencies must maintain records of their use of facial recognition services, develop an accountability report for that service, and allow for public comment on the accountability report.").

particular project or processing. They also inform public policymaking over the broader regulated area.[127]

The CPA's version of the impact assessment likely fits most squarely into the second model: risk-based collaborative governance. While there are benefits to this approach—for example, requiring companies to harness their own resources and expertise towards public ends—there are also significant potential pitfalls.

The most concerning potential pitfall is industry capture.[128] Impact assessments risk becoming self-interested and empty compliance processes if they are not accompanied by (a) public disclosure, (b) some input and/or oversight by impacted stakeholders or their representatives, and/or (c) meaningful government supervision coupled with a real threat of enforcement.[129]

The CPA's version of a DPA is "confidential" and explicitly exempted from public inspection and copying under the Colorado Open Records Act Pursuant to Section 1309(4). This likely precludes public disclosure, which can serve as the strongest check against capture.

However, the Department could still act to involve impacted stakeholders and their representatives, whose interests run orthogonal to controllers'. The Department could do so by (a) involving particularly adversely impacted stakeholders in drafting its rules or guidance for all DPAs—as, for example, WA SB 5116 requires—and/or (b) requiring controllers to consult with impacted stakeholders and relevant experts during the DPA process itself.

It is becoming best practice to ensure that controllers take into account external voices in assessing potential risks and harms. For example, the GDPR's DPIA encourages the consultation of external stakeholders.[130] In the United States, the recently introduced Algorithmic Accountability Act of 2022 ("AAA") would require covered entities:

> . . . to *meaningfully consult* (including through participatory design, independent auditing, or soliciting or incorporating feedback) with *relevant internal stakeholders* (such as employees, ethics teams, and

---

[127] *See* Selbst, *supra* note 114 at 174.

[128] *See* Waldman, *supra* note 111 at 5, 46; Kaminski, *supra* note 123 at 1533-34.

[129] *See* Kaminski, *supra* note 123 at 1532; *see also* Margot Kaminski, *Understanding Transparency in Algorithmic Accountability* (June 8, 2020) (forthcoming in Cambridge Handbook of the Law of Algorithms, ed. Woodrow Barfield, Cambridge University Press (2020)., Univ. of Colo. L. Legal Studies Rsch. Paper No. 20-34), https://ssrn.com/abstract=3622657.

[130] *DPIA Guidelines, supra* note 115 at 15.

> responsible technology teams) *and independent external stakeholders* (such as representatives of and advocates for impacted groups, civil society and advocates, and technology experts) as frequently as necessary.[131]

A model DPA "should better involve and engage impacted individuals, not just through surveys but through representative boards, before [a system] is deployed."[132] Accordingly, the AAA requires that controllers:

> Identify and describe any consultation with relevant stakeholders as required by section 3(b)(1)(G), including by documenting—
>
> (A) the points of contact for the stakeholders who were consulted;
>
> (B) the date of any such consultation; and
>
> (C) information about the terms and process of the consultation, such as—
>
> (i) the existence and nature of any legal or financial agreement between the stakeholders and the covered entity;
>
> (ii) any data, system, design, scenario, or other document or material the stakeholder interacted with; and
>
> (iii) any recommendations made by the stakeholders that were used to modify the development or deployment of the automated decision system or augmented critical decision process, as well as any recommendations not used and the rationale for such nonuse.[133]

This language represents one potential source that the Department could draw from in drafting accountability rules for the CPA's DPA requirement.

---

[131] S.3572, 117th Congress (2021-2022): *Algorithmic Accountability Act of 2022* , https://www.congress.gov/bill/117th-congress/senate-bill/3572/text. (emphasis added).

[132] Kaminski & Malgieri*, supra* note 112 at 139.

[133] Algorithmic Accountability Act of 2022, *supra* note 131 at Section 4(a)(2).

2.2. What Should Be In a DPA?

The Department should consider instituting requirements for the content of a DPA—including as an ongoing process. Any effective DPA "must ask open-ended questions, inviting bottom-up explanations."[134] In a bottom-up reporting structure, the DPA would "require the designers to explain their decisions" rather than "ask if specific checks were completed, like an audit might."[135] As an example, the DPA could "instruct the assessor to, among other things, '*rigorously explore and objectively evaluate all reasonable alternatives*.'"[136]

Accordingly, one possible model would prompt controllers to:

> "Envision [the]system and its role in society, considering:
>
> - System purpose, including key objectives and intended uses or applications . . .
> - Sensitive, premature, dual, or adversarial uses or applications . . . - Expected deployment contexts (e.g., geographic regions, time periods)
> - Expected stakeholders (e.g., people who will make decisions about system adoption, people who will use the system, people who will be directly or indirectly affected by the system, society), including demographic groups (e.g., by race, gender, age, disability status, skin tone, and their intersections)
> - Expected benefits for each stakeholder group, including demographic groups
> - Relevant regulations, standards, guidelines, policies, etc."[137]

Currently employed models support a reasonably broad scope of assessments. For example, environmental law in the United States requires impact asessments to be: " *analytic rather than encyclopedic*," "*discussed in proportion to their significance*," and "*no longer than absolutely necessary* to comply with" the statute and

---

[134] Selbst, *supra* note 114 at 148.

[135] *Id.*

[136] *Id.* (emphasis added).

[137] *Id.* at 183.

regulations.[138] The DPIA requirement of the GDPR[139] envisions a "similarly expansive scope of work to the NEPA model," including a "systematic description" of the processing, justifications, and plans for mitigation.[140] These guiding principles could similarly guide and enhance the DPA process under the CPA.

By comparison, the Canadian model for an algorithmic impact assessment (AIA) is based on a questionnaire that lacks flexibility. The questions it asks are "fixed and quite general."[141] This top-down approach prevents companies from ongoing reflection and examination that would prompt new questions and development; such an approach could stifle much-needed capacity for evolution in the assessment process.

Considering DPA rulemaking under these various models, with the goal of establishing the requirement as an ongoing, dynamic process, would not only protect the efficacy of the DPA requirement, but would also effectuate the controller duties listed in Section 1308. In particular, the duties of data minimization, purpose specification, and the duty to avoid secondary use remain in need of meaningful implementation, and naturally resonate with the framework and goals of a DPA. For example, the application of the duty of purpose specification in a DPA could both guide the DPA process and provide helpful documentation for both an entity and its regulator to understand its data streams. An effective DPA could identify the bounds of use to prevent function creep and effectuate data minimization, particularly where those secondary uses pose more risk to consumers.

2.3. Spot-Checking and Enforcement

Data Protection Authorities "must be willing to spot check and enforce against captured versions"[142] of submitted DPAs. This will be a crucial operational component of the CPA to prevent the DPA from becoming a mere compliance checklist.

---

[138] *See* 40 C.F.R. § 1502.2 (2020) (emphasis added). While the notice-and-comment structure under NEPA is incompatible with the confidentiality protected under the CPA, we include these requirements because they reflect strong guiding principles for impact assessments that inhere across regulatory regimes and areas of law. As noted *infra*, note 140 and accompanying text, these principles have already been applied to privacy law under the GDPR and are readily available for application under the CPA.

[139] Commission Regulation 2016/679 of Apr. 27, 2016, *General Data Protection Regulation,* art. 35(1), 2016 O.J. (L 119) 53.

[140] Selbst, *supra* note 114 at 144.

[141] *Id.* at 148.

[142] Kaminski & Malgieri, *supra* note 112 at 144.

First, spot-checking works to "monitor and improve the efficacy of the [DPA] process"[143] by acting as a potential sanction mechanism that may or may not be formal. More importantly, however, spot checking would allow the Department to "identify substantive problems" with data collection practices broadly, which over time, could then be learned from to "establish more concrete best practices or support the establishment of sector-specific codes of conducts around [data collection] fairness."[144]

To this end, the Department could "dictate minimum substantive standards for desired outcomes, while treating everything in excess as a governance problem."[145] To set these standards, the Department could consider "what harms even get counted as impact worth discussing"[146] and then work towards addressing them in the rules.

In doing so, the Department could consider on-the-ground feedback from controllers on strengths and weaknesses of existing DPIA requirements under the GDPR.[147] Controller feedback to the EDPS reveals both areas of lessons learned, where regulatory processes could provide for smoother guidance and certainty for regulated entities, as well as predictable areas where the Department can expect controller pushback for an easy compliance checklist.

The first lesson learned regarding EDPS guidance on when to conduct a DPIA promotes regulatory clarity and, as much as possible, simplicity. Controllers asked for "simplification of the procedure and the way the [guidance] document is drafted in view of its target audience."[148] Specifically, the controllers stated:

> If the Document is addressed to a wide variety of Controllers, the language used should be one that all non-practitioners should be able to understand. We need to keep in mind the audience: heads of unit/Directors who want to comply with the Regulation, but we would

[143] *Id.*

[144] *Id.*

[145] Selbst, *supra* note 114 at 168.

[146] *Id.*

[147] In 2020, the European Data Protection Supervisor (EDPS) conducted an EU-wide survey to solicit controller feedback on complying with the DPIA requirement under the GDPR. *EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation,* EDPB (2020), https://edps.europa.eu/sites/default/files/publication/20-07-06_edps_dpias_survey_en.pdf ("*EDPS Survey on DPIAs"*).

[148] *Id.* at 19

> rather have clear guidance in *less legalistic language* on how to be accountable and transparent.[149]

Other controllers offered "insight into where they would expect additional examples," saying that the EDPS guidance:

> . . . could provide *more details on dealing with existing processing operations*, and on specific factors that may affect the decision on the need for the DPIA…the negative and positive list and the threshold assessment could contain more concrete, illustrative examples and counterexamples.[150]

Lastly, regarding the usefulness of guidance on how to conduct a DPIA, the controllers asked the EDPB to: "Harmon[ize] templates, checklists, tools & methodology; [Provide] common practical methodology and step-by-step templates with detailed instructions . . .; [Provide] more streamlined guidance, such as a checklist; . . . Reflect about the best methodology that could be used by [controllers]; . . . [Publish] one good example of a real DPIA (e.g. drafted by the EDPS) as opposed to one bad example of another DPIA; . . . and, [Provide] a shorter version/simplified [sic] of this document could be easier for controllers to follow."[151] These reflect the tension between useful, concrete guidance and overly prescriptive or rigid checklists that could hinder ongoing flexibility and prioritize the costs of compliance over its efficacy.

While crafting DPA rules certainly implicates awareness of the cost of compliance, the greater focus should be on establishing a meaningful DPA process as a resource to protect consumers and support regulatory enforcement, as well as aid controllers in understanding and improving their data practices. Similarly, DPA rulemaking has some of the strongest connection to determining whether controller duties will truly be effectuated. These principled goals, more than the ease afforded by a template, should take priority in adopting DPA rules.

---

[149] *Id.* (emphasis added).

[150] *Id.* at 19-20. (emphasis added). This also illustrates the strength and utility of the European approach where it has provided illustrative examples along with guidance. *Compare DPIA Guidelines, supra* note 115 *with Guidelines on the Territorial Scope of the GDPR*, EDPB, (Nov. 12, 2019), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.)

[151] *EDPS Survey on DPIAs*, *supra* note 147, at 21–22.

3. Internal Processes for Consumer Requests & Appeals

Internal governance surrounding receiving and responding to consumer requests and appeals will have significant practical effect upon the overall strength and success of the Colorado Privacy Act (CPA).

The consumer rights outlined in Section 1306 may be exercised only by submitting a consumer request to a controller.[152] As a result, organizations may make consumer rights ineffective as a practical matter if the process for submitting a request is too arduous. The openness of the Act leaves room for this to occur intentionally, through companies imposing barriers; or unintentionally, for lack of clear and effective internal procedures. Either way, the effect is nullification of consumer rights as a practical matter.[153] Therefore, the processes for requests and appeals will determine the efficacy of the CPA's consumer rights in Section 1306.

Currently these rights are vague and open; however, the recent passage of Connecticut's Privacy Act allows for strong alignment between Colorado, California, Connecticut, and, in some respects, the GDPR.[154] The Department has the opportunity to strengthen consumer rights through rulemaking regarding internal data governance requirements and procedures to facilitate methods of receiving and responding to requests and appeals. This rulemaking could focus either on tracking with California as the current U.S. benchmark for requiring specific business practices, aligning with Connecticut, or raising the bar further.

This section therefore discusses the importance of internal governance to effectuate consumer rights by ensuring controllers can and do respond to them. It also briefly discusses ancillary issues that could stymie exercise of rights prior to the function of internal governance, particularly in the areas of submitting requests in the first place and exploitation of statutory exceptions.

3.1 Internal Governance to Strengthen Response to Requests

At the heart of successful provision of effective consumer rights lies a data governance structure for organizations to process consumer requests to exercise

---

[152] C.R.S. § 6-1-1306(1) (2021).

[153] Internal company processes for contesting automated decisionmaking raise similar concerns as to whether consumer rights implemented by (or delegated to) companies will be effective in practice. Margot E. Kaminski and Jennifer M. Urban, *The Right to Contest AI*, 121 Colum. L. Rev 1957, 2003–46 (2021), https://columbialawreview.org/wp-content/uploads/2021/11/Kaminski-Urban-The_Right_to_Contest_AI.pdf.

[154] *See* David Stauss, *Connecticut Legislature Passes Consumer Privacy Act*, Byte Back (Apr. 28, 2022), https://www.bytebacklaw.com/2022/04/connecticut-legislature-passes-consumer-privacy-act.

rights. The goal is to provide enough clear structure and procedure to foster transparency and accountability while maintaining flexibility.[155] The open requirements provided by the Act lend too easily to industry self-certification. Internal governance structures do not have to be burdensome or complex and, once established, can rely on the routine of established processes and forms and other mechanisms.[156]

Generally, the CPA includes fairly light requirements for responding to requests—authentication of requests, setting lengthy timelines to process and respond to requests and appeals, [157] and requiring "explanation" when a company issues an extension or denial.[158] These statutory requirements are open enough for rulemaking to provide practical parameters, but leave the efficacy of rights open and vulnerable without rules.

In particular, the statutory requirements at Sections 1306 and 1308 address the end result of a consumer request—what responses an organization must undertake, and within what timeframe—it leaves open how an organization will get there. Internal governance must bridge the gap[159] as to how companies will receive requests, compile them from various intake sources, authenticate requests, review them to determine if they may or must be processed or declined according to the CPA and other legal obligations, carry out the request when approved in regards to

---

[155] *See generally*, Hou, Bohan, *A Novel Data Governance Scheme Based on the Behavioral Economics Theory* (January 27, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773565.

[156] *How to Choose the Right Privacy Governance*, Data Privacy Manager, GDPR Blog (Aug. 3, 2021), https://dataprivacymanager.net/gdpr-compliance-privacy-governance-model/; *Choosing the Right Privacy Governance Tool for Your Organization*, Focal Point Insights (Jan. 28, 2020), https://blog.focal-point.com/choosing-the-right-privacy-governance-tool-for-your-organization; *compare* Margot E. Kaminski, *The Case for Data Privacy Rights (Or 'Please, a Little Optimism')* Notre Dame Law Review online, Forthcoming, Univ. of Colo. L. Legal Studies Rsch. Paper No. 22-7 ((March 11, 2022), https://ssrn.com/abstract=4055627
and Binary Governance, *supra* note 123, *with* Salomé Viljoen, *A Relational Theory of Data Governance*, 131 Yale L. J. 573 (2021), https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance. e

[157] C.R.S. § 6-1-1306(2)(a (2021).

[158] *Id.*

[159] Heather Federman & Peggy Tsai, *What Lives Between Data Privacy and Data Governance? Bettter Compliance*, IAPP (Apr. 28, 2020), https://iapp.org/news/a/what-lives-between-data-privacy-and-data-governance-better-compliance.

collected data, and respond back to the consumer.[160] Compilation capabilities will be particularly important, both to establish a single queue for processing requests regardless of how they were submitted (for example, by phone, email, or online form) and to identify personal data across the various areas it may be stored and used within an organization across departments, storage, and uses.

Further, personal data must be accessible across these various stores and uses—data correction, for example, must occur in all data flows and repositories to be effective and meaningful. This means that both personal data and an organization's data processes must be categorized, accessible, and modifiable at sufficiently specific levels for data to be identified, accessed, and processed accordingly. This can include mapping data storage and data flows (processing) to identify where personal data is located and how it is used.[161]

To do so, the Department could implement the request and appeals process in any number of ways. On its face, the CPA merely requires an appeals process,[162] without dictating a timeline or the substance on which a decision might be appealed. The Department could choose to implement a more granularized procedure with a more precise suggested timeline. The Department could choose to more clearly articulate the substantive basis of consumer appeals, and limit the exceptions companies might rely on in rejecting rights (such as trade secrecy), discussed *infra*. As shown in the diagram below with current examples, there are at least four archetypes of consumer contestation that arise from a matrix reflecting the intersection of a procedural focus or a substantive focus, and a framework based more on standards or rules.[163]

---

[160] *A Guide to Consumer Rights Request Management*, Collibra, https://www.collibra.com/us/en/resources/consumer-rights-request (describing the four "Rs" of responding to requests: Receive, Review, Retrieve, Respond).

[161] *Id.* (Identifying the problems of "fragmented data and application architectures," unknown data flows, and insufficiently granular control, and recommending "PI discovery and classification" to identify data and a "process register" to map data flows); *see also* GDPR Art. 30 (setting out requirements for records of processing activities); GDPR Recital 82 ("In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it…for monitoring….).

[162] C.R.S. § 6-1-1306(3) (2021). Submitting the appeal must be "conspicuously available" and as easy to use as the process for submitting a request. *Id.* at § 6-1-1306(3)(a). However, without guidelines around how easy it must be to submit a request, this effectively permits appeals to be as difficult to use as the process for submitting a request. *See infra* Section 3.2.

[163] Kaminski & Urban, *supra* note 153, at 2008–09. Table from *Id.* at 2011.

	Contestation Standard	*Contestation Rule*
Procedural Focus	1) The GDPR's "Right to Contestation"	2) The Digital Millennium Copyright Act's (DMCA's) "Notice-and-takedown" regime; The UK Right to Contestation
Substantive Focus	2) The EU's "Right to Be Forgotten" (RTBF); The Slovenian Right to Contestation	3) The Fair Credit Billing Act (FCBA); The French & Hungarian Rights to Contestation

Within the framework chosen by the Department, rules providing benchmarks to build an internal process framework could be as simple as identifying which employees have access to personal data, where the information is stored and what processes utilize it, and an assessment of whether current data flow structures permit accessing particular pieces of data.

Pending EDPB guidance could also inform Department rulemaking. The EDPB is currently developing guidance pertinent to internal governance procedures for the GDPR right of access, similar to the CPA rights of access and portability. In guidelines proposed in January 2022 and open for comment until mid-March, both the guidelines and comments explore detailed approaches for controllers to receive and respond to requests.[164] These include a combination of procedural and substantive requirements, including identification and documentation to support internal processes, topics that should be addressed in response to requests, and the level of detail of responses. Alternatively, governance structures could borrow from already-established compliance regimes, such as those established in the healthcare and finance industries.

Finally, while most rules will likely establish a floor for compliance, some should also establish a practical ceiling. For example, the CPA currently lacks a lookback period bounding access and portability requests, leaving open the amount of time over which it must account for the collection and use of personal data. California sets the limit at the twelve months preceding the request;[165] Colorado could follow

[164] *Guidelines 01/2022 on Data Subject Rights – Right of Access*, EDPB (Jan. 28, 2022), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.

[165] Cal. Civ. Code 1.18.5 § 1798.130 (2021).

this example or consider a broader lookback period for a consumer's first request. In doing so, it should also keep an eye on Federal Trade Commission activity, as Chairwoman Kahn has suggested that her tenure may favor substantive requirements over procedural protections.[166]

3.2 Strengthening Methods of Receiving Requests

For successful robust internal governance processes to effectuate consumer rights, consumers must be able to successfully submit requests to exercise rights. Receiving requests implicates both the number and types of methods of requests companies accept, as well as their accessibility and ease of use by consumers. Further, methods to receive opt-out requests carries some different implications than the exercise of other rights, such as access and portability, that should be reflected in the processes for receiving those requests.

The CPA sets out broad and basic requirements for receiving consumer requests. A controller must identify the methods of request via which consumers may submit requests to exercise rights in its privacy policy.[167] This specification must include the controller's contact information and how consumers may submit requests and appeals.[168] The only other concrete statutory requirement is around the use of consumer accounts to submit requests: while a controller may require a consumer to submit a request through an already-existing account, it may not require a customer to create an account to submit a request.[169]

Unlike the CCPA and CPRA,[170] the CPA does not require any minimum number or type of method for requests, with the notable exception of opt-out rights. Rulemaking relating to the methods of the request should consider some general principles, including minimum threshholds, for providing effective methods of

---

[166] Andrea Vittorio, *FTC Chair Calls for Shift from 'Overwhelming' Privacy* Policies, Bloomberg Law (Apr. 11, 2022, 5:58 PM), https://news.bloomberglaw.com/privacy-and-data-security/ftc-chair-calls-for-shift-from-overwhelming-privacy-policies.

[167] C.R.S. §§ 6-1-1306(1), 1308(1)(a)(III) (2021).

[168] C.R.S. § 6-1-1308(1)(a)(III) (2021).

[169] C.R.S. § 6-1-1306(1), 1308(c)(I) (2021).

[170] Cal. Civ. Code 1.18.5 § 1798.130 (2021) (requiring at least two methods for submitting each type of request, one of which must be a toll-free number for requests to know; one of which must be via the website if the company has one; and one of which must be specified links on the website to opt out of sale and sharing and to limit use and disclosure of sensitive information.) The CCPA regulations also require businesses to respond to requests submitted that do not conform to the designated methods, by either processing the request as if submitted via a designated method or directing the consumer to the designated methods. CCPA Regulations, 11 C.C.R § 999.312(e) (2021).

requests regarding any and all rights. It should also consider particular practical and statutory demands for effective methods of request to exercise opt-out rights.

3.2.1. Minimum Thresholds for Any Request

The statute offers guidance that the designated methods of request "must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication relating to the request, and the ability of the controller to authenticate the identity of the consumer making the request."[171]

While these requirements nod to common interactions over the internet, approaches in the GDPR, and practices managing data security and identity verification, they do not address concrete application. On its face, the statute permits a method of request via anything from a user-friendly online form to an email to paper mail to fax to in-person dropoff.

The Department could therefore establish rules for minimum permissible methods for submitting requests, such as following California's approach of requiring an organization with a website to receive requests via the website. While simple, the California requirement for a business to include an opt-out link on its website has been a powerful tool to facilitate consumer exercise of rights and evaluate compliance. It has also proven a surprising challenge, as many websites are still working to provide these links,[172] suggesting that explicit requirements or examples of acceptable methods of request could be beneficial.

3.2.2. Methods of Request for Opt-out Rights

Rules for methods to request exercise of opt-out rights carry particular weight both because they relate to central rights around sale of personal data, targeted advertising, and profiling, and because consumers may exercise them more commonly than other rights such as the rights of data accessibility and portability.

In particular, rulemaking could preemptively protect consumers' ability to exercise opt-outs rights via an agent, including a browser setting, global device setting, or universal opt-out mechanism. Because an organization must be able to authenticate the identity of every consumer request, including opt-outs and opt-outs via an agent,[173] the Act could currently present a conflict where a setting or universal opt-out may not clearly permit authentication. The rules therefore could establish that

---

[171] *Id.* at § 6-1-1306(1).

[172] Ben Kimberly & David Zetoony, *Data Privacy Requests Metrics: Lessons for Your Privacy Program*, IAPP (Sept. 16, 2021), https://iapp.org/news/a/data-privacy-requests-metrics-lessons-for-your-privacy-program/

[173] Cf. Cal. Civ. Code 1.18.5 § 1798.130 (2021) (requiring authentication only for requests to know, correct, and delete).

universal or setting-based opt-outs presumptively satisfy authentication requirements, or include authentication capability in the rules for acceptable opt-out mechanisms or settings. Similarly, rules for authentication for all opt-outs—a one-way message to controllers—might carry a much lower authentication requirement than exercise of other rights that require substantive response and disclosure from controllers back to consumers.

3.3 Minimizing Exploitation of Exceptions

The Department should consider rulemaking that limits predictable exploitation of statutory exceptions. In particular, it should bound exceptions for technical feasibility, trade secret, and consent that overrides a universal opt-out.

The exception to the rights of access and data portability that a controller must only provide the consumer's data in a readily usable format "to the extent technically feasible" would naturally be bounded by reasonable internal governance requirements, discussed *supra*. A governance framework for identifying, classifying, locating, and retrieving or modifying data would not only prevent the technical feasibility exception from undermining the rights—in effect, using lack of internal governance to claim technical infeasibility—but would significantly strengthen the rights and guide companies in establishing workable, compliant data management.

Second, rulemaking could address growing opposition to disclosure on the basis of trade secrets. Companies already argue that their manner of constructing consumer profiles (i.e., proprietary algorithms) is a trade secret and, thus, that consumer profiles—some of the information this Act most seeks to shed light upon—are exempt from disclosure. This has already caused enough contention to be the subject of the only Attorney General opinion interpreting the CCPA, released March 10, 2022, concluding that inferences generated about a consumer via a secret algorithm may not automatically be withheld under trade secret protection.[174]

The open language in the CPA, in contrast to the prescriptions of the CCPA, makes it more vulnerable to sweeping trade secret claims of exemption.[175] In addition to the proprietary algorithm argument addressed by the California Attorney General, other passed and proposed state legislation with language more similar to the CPA has revealed strategies to leverage trade secret to avoid meaningful disclosure. The Utah Privacy Act requires disclosure only of data provided by the consumer (not,

[174] Cal. Att'y Gen. Op. No. 20-303 (Mar. 10, 2022), https://oag.ca.gov/opinions/monthly-report.

[175] C.R.S. § 6-1-1306(1)(e) (2021) ("Nothing in this subsection 1(e) requires a controller to provide the data to the consumer *in a manner* that would disclose the controller's trade secrets.") (emphasis added).

for example, information provided by a data broker about the consumer),[176] while one proposed bill in Indiana would have considered the access right satisfied by a "representative summary"[177]—i.e., a uniform generic list—of the kinds of information possessed regarding a consumer rather than the specific data itself.

Under the language of the CPA, a company could assert compliance with the access right if it combined these approaches, disclosing routine information provided by the consumer and glossing over more detailed or pernicious information by providing a generic list of kinds of data generated or processed by algorithms once purchased, on trade secret grounds. Rulemaking, therefore, could clarify that the trade secret protection does not extend to the data produced by processes that may fall under trade secrets—that the inferences produced by an algorithm cannot be withheld because their disclosure is not "in a manner" that discloses the trade secret itself—i.e., the algorithm.

Finally, the CPA's exception permitting specific consent to override a universal opt-out signal[178] leaves a problematic chronological loophole. Under the statutory language, an entity could obtain the go-ahead from users now to collect data for sale or targeted advertising—for example, through failure to opt-out of default terms set out in its privacy policy. It could then assert that this acceptance, obtained prior to accepting a universal opt-out signal, constitutes consent that overrides the universal opt-out signal once it accepts it by July 1, 2024, and decline to recognize the universal opt-out signal on that ground from its inception. Such an interpretation could defeat the intended ease and widespread benefit of the universal opt-out provision. The Department could address this issue through rulemaking by clarifying that consent—or at least passive acceptance—to collection of information obtained by an organization prior to July 1, 2024 would not take precedence over a later attempt to opt-out via a universal opt-out mechanism.

4. Additional Areas for Consideration in Formal Rulemaking

While this submission has focused primarily on notice, data protection assessments, and consumer requests, this section highlights some other areas deserving significant consideration during rulemaking.

Sensitive Data and Inferences. First, the language of the CPA in Section 1308(7) requiring consent to process sensitive data, as well as the definition of consent in Section 1303(5), leave open rulemaking regarding inferences of sensitive information. The language of the statute allows rulemaking to clarify that consent required for processing sensitive information includes sensitive information

---

[176] Utah Code Ann. § 13-61-201(3) (LexisNexis 2022, effective 2023).

[177] *E.g.*, Indiana proposed S.B. 358(3)(1)(b)(4)(B), http://iga.in.gov/legislative/2022/bills/senate/358.

[178] C.R.S. § 6-1-1306(a)(IV)(C) (2021).

generated by inference. It could apply to inferred sensitive data generated from non-sensitive data, including data the processor did not collect itself. As a result, not only would consumers be contacted for consent regarding sensitive data they were unaware was collected via inferences, but would gain visibility into which controllers and processors—including those with which they did not directly interact—are utilizing it.

Effectuating Controller Duties. Second, although we have mentioned the importance of controller duties in the context of specific areas of potential rulemaking, the importance of effectuating these duties across areas of rulemaking cannot be understated. Not only do these duties require rulemaking to become effective, but they provide key guiding principles for the other provisions of the CPA and therefore can guide rulemaking. For example, implementation of the duty of purpose specification could inform rulemaking around notices, defining a clear and affirmative act of consent, as well as properly responding to a request.

Automated Decisionmaking Processes. Finally, as reflected in the CPA[179] and the work of scholars[180] and regulators,[181] the role of automated decisionmaking processes (ADP) plays an important and increasing role in data management and data privacy. Again, while this is outside the scope of this submission, we urge the Department to keep in mind the role of ADPs in its formal rulemaking this fall.

---

[179] C.R.S. §6-1-1303(20) (2021).

[180] Rebecca Crootof and Margot E. Kaminski & William Nicholson Price II, *Humans in the Loop* Univ. of Colo. L. Legal Studies Research Paper No. 22-10, U of Michigan Public Law Research Paper No. 22-011, (March 25, 2022) (forthcoming in Vanderbilt Law Review, 2023), https://ssrn.com/abstract=4066781; Margot E. Kaminski, *The Right to Explanation, Explained*, 34 Berkeley Tech. L. J. 189 (2019), https://btlj.org/data/articles2019/34_1/05_Kaminski_Web.pdf.

[181] Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FTC Business Blog (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (providing links to FTC resources including business guidance on algorithms, a report on big data and machine learning, and a hearing on algorithms and AI); Article 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679*, WP251 (rev'd Aug. 22, 2018), https://ec.europa.eu/newsroom/article29/items/612053/en.

Appendix A: Sources for Notice

(in order of appearance)

Idris Adjerid, Alessandro Acquisti, & George Lowenstein, *Choice Architecture, Framing, and Cascaded Privacy Choices*, Management Science 65(5) 1949-2443 (2019), https://ssrn.com/abstract=2765111

Hana Habib, Yixin Zou, Adliti Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lori Cranor, Norman Sadeh, & Florian Schaub, *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, USENIX Proceedings of the Fifteenth Symposium on Usable Privacy and Security 387 (2019), https://www.usenix.org/system/files/soups2019-habib.pdf

Article 29 Data Protection Working Party, *Guidelines on Consent Under Regulation 2016/679,* EDPB (May 4, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf ("*Guidelines on Consent*")

Article 29 Data Protection Working Party, *Guidelines on Transparency Under Regulation 2016/679*, EDPB (Apr. 11, 2018), https://ec.europa.eu/newsroom/article29/items/622227 ("*Guidelines on Transparency*")

Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (2018)

Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor, *A Design Space for Effective Privacy Notices*, Usenix (Symposium on Usable Privacy and Security) (July 2015), https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

Lorie *Faith Cranor*, Carnegie Mellon Univ., https://www.cmu.edu/epp/people/faculty/lorrie-faith-cranor.html

Mobile Privacy Disclosures: Building Trust Through Transparency, FTC (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf

Mobile Health App Developers: FTC Best Practices, FTC (Apr. 2016), https://www.ftc.gov/business-guidance/resources/mobile-health-app-developers-ftc-best-practices

A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers, FTC (Staff Report) (Oct. 21, 2021), https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-

you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf

Lesley Fair, *What Vizio was Doing Behind the TV Screen*, FTC Bus. Blog (Feb. 6, 2017), https://www.ftc.gov/business-guidance/blog/2017/02/what-vizio-was-doing-behind-tv-screen

VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent, FTC (Feb. 6, 2017), https://www.ftc.gov/news-events/news/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it-collected-viewing-histories-11-million

CCPA Regulations, 11 C.C.R. §300 et seq. (2021), https://oag.ca.gov/privacy/ccpa/regs

Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper, *Harder to Ignore? Revisiting Pop-up Fatigue and Approaches to Prevent It*, Symposium on Usable Privacy and Security (July 2014), https://www.usenix.org/conference/soups2014/proceedings/presentation/bravo-lillo

M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1027 (2013), http://scholarship.law.nd.edu/ndlr/vol87/iss3/3

A Conversation with Colorado Attorney General Phil Weiser, Data Privacy Unlocked: Legislating Data Privacy Series (May 9, 2022), available via major podcast platforms or at https://www.bytebacklaw.com/2022/05/legislating-data-privacy-series-a-conversation-with-colorado-attorney-general-phil-weiser

An Act Concerning Personal Data Privacy and Online Monitoring, Pub. Act No. 22-15 (2022), https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022

Webinar: Analyzing the Connecticut Data Privacy Act, Byte Back (May 2, 2022), https://www.bytebacklaw.com/2022/05/webinar-analyzing-the-connecticut-data-privacy-act

Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, & Arvind Narayanan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. 3, CSCW 81, 2 (2019), https://doi.org/10.1145/3359183

Arunesh Mathur, *Dark Patterns at Scale: Findings from a Crawl of 11k Shopping Websites*, slide 9 (2019), http://aruneshmathur.co.in/files/talks/CSCW19_DarkPatterns_Slides.pdf

Arunesh Mathur, Jonathan Mayer, & Mihir Kshirsagar, *What Makes a Dark Pattern…Dark? Design Attributes, Normative Considerations, and Measurement Methods* (Jan. 13, 2021), https://arxiv.org/abs/2101.04843

Jake Holland, *Amazon Alexa Suit's Registered User Wiretap Claims Axed*, Bloomberg Law (May 9, 2022), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X72JHUV8000000?bna_news_filter=privacy-and-data-security#jcite

Enforcement Policy Statement Regarding Negative Option Marketing, FTC 13 (Nov. 4, 2021), https://www.federalregister.gov/documents/2021/11/04/2021-24094/enforcement-policy-statement-regarding-negative-option-marketing

Cookies Equally Easily Accepted or Refused: the CNIL Sends a Second Series of Orders to Comply, CNIL (July 23, 2021), https://www.cnil.fr/en/cookies-equally-easily-accepted-or-refused-cnil-sends-second-series-orders-comply

CNIL's New Guidelines and Recommendations on Cookie Consent, CookieYes (July 14, 2021), https://www.cookieyes.com/blog/cnil-guidelines-and-recommendations-on-cookie-consent

GDPR: Consent, GDPR-Info, https://gdpr-info.eu/issues/consent (last accessed May 16, 2022)

FTC to Ramp Up Enforcement Against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions, FTC Press Release (Oct. 28, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions

Lior Strahilevitz and Jamie Luguri, *Shining a Light on Dark Patterns*, 13 U of Chic. J. of L. Analysis, Pub. L. Working Paper No. 719 44 (2021), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/shining-a-light-on-dark-patterns.pdf

Bringing Dark Patterns to Light, FTC (Apr. 29, 2021), https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop (providing links to agenda, papers, and comments)

Jennifer King & Adriana Stephan*, Regulating Privacy Dark Patterns in Practice—Drawing Inspiration from California Privacy Rights Act*, 5 Geo. L. Tech. Rev. 251, 263 (2021), https://georgetownlawtechreview.org/wp-content/uploads/2021/09/King-Stephan-Dark-Patterns-5-GEO.-TECH.-REV.-251-2021.pdf

Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognize and avoid them, EDPB (Adopted on Mar. 14, 2022), https://edpb.europa.eu/system/files/2022-03/edpb_03-

2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf ("Guidelines on Dark Patterns")

Shaping Choices in the Digital World, CNIL (Jan. 2019), https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

CNIL Fines Google €50 Million for Alleged GDPR Violations, Hunton Privacy Blog (Jan. 23, 2019), https://www.huntonprivacyblog.com/2019/01/23/cnil-fines-google-e50-million-for-alleged-gdpr-violations

Appendix B: Sources for Data Protection Assessments

(in order of appearance)

Cal. Civ. Code til. 1.81.5, California Consumer Privacy Act of 2018 (2022), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Ari Waldman, *Privacy, Practice, and Performance*, 110 Cal. L. R. 1 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784667

Margot Kaminski & Gianclaudio Malgieri, *Algorithmic impact assessments under the GDPR: producing multi-layered explanations*, 2 Int. Data Privacy L. 11 125, 138 (2021), https://academic.oup.com/idpl/article_/11/2/125/6024963

Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 Harv. L. J. & Tech. 117, 118 (2021), https://jolt.law.harvard.edu/assets/articlePDFs/v35/Selbst-An-Institutional-View-of-Algorithmic-Impact-Assessments.pdf

Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679*, WP248 (Oct. 13, 2017), https://ec.europa.eu/newsroom/article29/items/611236/en

Risk Management, NIST, https://www.nist.gov/risk-management (last accessed May 17, 2022)

Margot Kaminski, *Regulating the Risks of AI*, BU Law Review (forthcoming 2023) (draft on file with author)

Cybersecurity Framework, NIST https://www.nist.gov/cyberframework (last accessed May 17, 2022).

AI Risk Management Framework, NIST, https://www.nist.gov/itl/ai-risk-management-framework (last accessed May 17, 2022).

Margot Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529 (2019), https://scholar.law.colorado.edu/articles/1265.

Wash. S. Rep. No. 5166 (2021), https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bill%20Reports/Senate/5116%20SBR%20SGE%20TA%2021.pdf.

S.3572 117th Congress (2021-2022): Algorithmic Accountability Act of 2022, https://www.congress.gov/bill/117th-congress/senate-bill/3572/text.

Margot Kaminski, *Understanding Transparency in Algorithmic Accountability* (June 8, 2020) (forthcoming in Cambridge Handbook of the Law of Algorithms, ed.

Woodrow Barfield, Cambridge University Press (2020)., U of Colorado Law Legal Studies Research Paper No. 20-34), https://ssrn.com/abstract=3622657

Commission Regulation 2016/679 of Apr. 27, 2016, *General Data Protection Regulation,* art. 35(1), 2016 O.J. (L 119) 53, https://gdpr-info.eu

EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation, EDPB (2020), https://edps.europa.eu/sites/default/files/publication/20-07-06_edps_dpias_survey_en.pdf

Appendix C: Sources for Internal Processes for Consumer Requests and Appeals

(in order of appearance)

David Stauss, *Connecticut Legislature Passes Consumer Privacy Act*, Byte Back (Apr. 28, 2022), https://www.bytebacklaw.com/2022/04/connecticut-legislature-passes-consumer-privacy-act

Heather Federman & Peggy Tsai, *What Lives Between Data Privacy and Data Governance? Bettter Compliance*, IAPP (Apr. 28, 2020), https://iapp.org/news/a/what-lives-between-data-privacy-and-data-governance-better-compliance

A Guide to Consumer Rights Request Management, Collibra, https://www.collibra.com/us/en/resources/consumer-rights-request

Margot Kaminski and Jennifer M. Urban, *The Right to Contest AI*, 121 Colum. L. Rev 1957, 2003–46 (2021), https://columbialawreview.org/wp-content/uploads/2021/11/Kaminski-Urban-The_Right_to_Contest_AI.pdf

Ben Kimberly & David Zetoony, *Data Privacy Requests Metrics: Lessons for Your Privacy Program*, IAPP (Sept. 16, 2021), https://iapp.org/news/a/data-privacy-requests-metrics-lessons-for-your-privacy-program/

Cal. Att'y G.n Op. No. 20-303 (Mar. 10, 2022), https://oag.ca.gov/opinions/monthly-report

Hou, Bohan, *A Novel Data Governance Scheme Based on the Behavioral Economics Theory* (January 27, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773565

How to Choose the Right Privacy Governance, Data Privacy Manager, GDPR Blog (Aug. 3, 2021), https://dataprivacymanager.net/gdpr-compliance-privacy-governance-model

Choosing the Right Privacy Governance Tool for Your Organization, Focal Point Insights (Jan. 28, 2020), https://blog.focal-point.com/choosing-the-right-privacy-governance-tool-for-your-organization

Margot E. Kaminski, *The Case for Data Privacy Rights (Or 'Please, a Little Optimism')* Notre Dame Law Review online, Forthcoming, U of Colorado Law Legal Studies Research Paper No. 22-7 ((March 11, 2022), https://ssrn.com/abstract=4055627

Margot Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529 (2019), https://scholar.law.colorado.edu/articles/1265

Salomé Viljoen, *A Relational Theory of Data Governance*, 131 Yale L. J. 573 (2021), https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance.