Suggested Enhancements to "Commission-Approved Compliance Guidelines" in the American Privacy Rights Act

A Policy Note from the Centre of Information Policy Leadership (CIPL)[1]
June 11, 2024[2]

On April 7, 2024, Senate Commerce Committee Chair Maria Cantwell and House Energy and Commerce Committee Chair Cathy McMorris Rodgers released a discussion draft of the American Privacy Rights Act (APRA), a comprehensive federal consumer privacy framework built on prior congressional efforts including the American Data Privacy and Protection Act (ADPPA). On May 21, 2024, Rep. Rodgers along with House Commerce Subcommittee Chair Gus Bilirakis (R-FL) released a second discussion draft. The analysis in this policy note is based on the May 21 draft.

The Centre for Information Policy Leadership (CIPL) offers the following suggestions to enhance the effectiveness of **APRA Section 115: "Commission-Approved Compliance Guidelines":**

- **Streamline the approval process to align with widely recognized certification schemes, and**
- **Expand the availability of Compliance Guidelines to all entities.**

CIPL has long supported flexible, co-regulatory mechanisms—such as codes of conduct, certifications, and accountability standards—and we are encouraged to see APRA's inclusion of "Compliance Guidelines" in its provisions.[3]

As currently drafted, however, the proposal fails to embrace the full potential that certification schemes can bring. **The Annex to our note sets forth specific suggested edits in redline** that would advance the twin goals of streamlining interoperability with other privacy frameworks and making the Compliance Guidelines more broadly available.

---

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member organizations. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this report should be construed as representing the views of any individual CIPL member or of the law firm of Hunton Andrews Kurth.

[2] For earlier CIPL recommendations on U.S. federal privacy legislation, see, for example, *Ten Principles for a Revised US Privacy Framework*, CIPL Policy Paper, March 21, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_principles_for_a_revised_us_privacy_framework__21_march_2019_.pdf.

[3] For purposes of our analysis, the proposed "Compliance Guidelines" are the functional equivalents or privacy marks, certifications and codes of conduct, as enabled in other privacy frameworks, such as the EU General Data Protection Regulation (GDPR) and the Global Cross-Border Privacy Rules (CBPR).

1. Streamlining the Approval Process

As currently drafted, APRA Sec. 115 requires entities to seek one-off approval of individual compliance guidelines from the FTC. CIPL, however, suggests a more efficient process—such as that advanced by the COPPA Rule[4] and by the Global Cross Border Privacy Rules System.[5] This process places the responsibility of obtaining approval for "compliance guidelines" (or certification programs) on the "independent organizations" (or "certification bodies") that administer these programs and then enables entities to obtain certification to these programs from the independent organizations by demonstrating their compliance with these programs. If revised in this manner, the provision would more closely align with the type of certification framework already familiar to the FTC in the COPPA context and already widely recognized by legal and privacy regimes around the world. The benefits of certification schemes are highlighted on the follow page.

2. Expanding access to <u>all</u> entities

As currently drafted, APRA Sec. 115 excludes certain covered entities—specifically data brokers and large data holders—from its scope. It also excludes service providers. This is a missed opportunity to leverage formal and enforceable accountability mechanisms that would facilitate compliance by all entities that APRA seeks to regulate. Importantly, allowing all entities to become certified would in no way affect the investigative and enforcement discretion of the FTC. Indeed, all stakeholders can benefit from making certifications available to these entities as well.

Given our extensive experience promoting organizational accountability and best practices, we welcome the opportunity to participate constructively in ongoing policy discussions regarding APRA. For additional information, please contact CIPL.

---

[4] Children's Online Privacy Protection Rule, 16 CFR part 312.

[5] See https://www.globalcbpr.org/ for information on Global Cross-Border Privacy Rules (CBPR) and Global Privacy Recognition for Processors (PRP).

Stakeholder benefits from formal accountability and compliance mechanisms like the "Commission-Approved Compliance Guidelines" in the American Privacy Rights Act

BENEFITS FOR REGULATORS:

- **Reduces oversight workload** because certification bodies take on and share the burdens of supervision and oversight.
- **Improves compliance** due to mandatory periodic re-certification processes and ongoing monitoring requirements.
- **Regulator enforcement augmented** by complaint-handling mechanisms provided for in the Compliance Guidelines
- **Transparency requirements** inform regulators of data practices.

BENEFITS FOR ENTITIES:

- **Facilitates compliance** with domestic and internationally recognized standards.
- **Assists SMEs** that lack the resources to devise their own comprehensive compliance programs.
- **Facilitates an entity's due diligence** when seeking third-party vendors, processors, and business partners.
- **Demonstrates compliance and accountability** via certification "trustmark."
- **Good faith compliance** can serve as a mitigating factor in enforcement contexts.

BENEFITS FOR INDIVIDUALS:

- **Strengthens privacy protections** for individuals.
- **Builds trust** with companies that are processing personal data.
- **Facilitates commerce** in the digital environment.

Annex

Section 115 Redline

SEC. 115. COMMISSION-APPROVED COMPLIANCE GUIDELINES.

(a) APPLICATION FOR COMPLIANCE GUIDELINE APPROVAL.—

(1) IN GENERAL.—An independent organization ~~covered entity that is not a data broker and is not a large data holder, or a group of such covered entities,~~ may apply to the Commission for approval of 1 or more sets of compliance guidelines that will be used to assess and certify activities by all covered entities (including large data holders and data brokers) as well as service providers, hereinafter "entity or entities", governing the collection, processing, retention, or transfer of covered data ~~by the covered entity or covered entities~~.

(2) APPLICATION REQUIREMENTS.—An application under paragraph (1) shall include—

(A) a description of the activities the proposed compliance guidelines are designed to cover and which specific requirements of this title those activities are designed to address;

(~~A~~B) a description of how the proposed guidelines will meet or exceed the specific requirements of this title identified under subparagraph (A);

~~(B) a description of the entities or activities the proposed guidelines are designed to cover;~~

~~(C) a list of the covered entities, to the extent known at the time of application, that intend to adhere to the proposed guidelines;~~

(~~D~~C) a description of how the ~~an~~ independent organization will maintain its independence from any entities it may assess for compliance with these guidelines~~, not associated with any of the intended adhering covered entities, that will administer the proposed guidelines~~; and

(~~E~~D) a description of how ~~such intended adhering~~ entities will be assessed and certified for adherence to the proposed guidelines~~ by the independent organization described in subparagraph (D)~~.

(3) COMMISSION REVIEW.—

(A) INITIAL APPROVAL.—

(i) PUBLIC COMMENT PERIOD.—Not later than 90 days after receipt of an application regarding proposed guidelines submitted pursuant to paragraph (1), the Commission shall publish the proposed compliance guidelines submitted as part of the independent organization's application and provide an opportunity for public comment on such proposed guidelines.

(ii) APPROVAL CRITERIA.—The Commission shall approve an application regarding proposed guidelines submitted pursuant to paragraph (1)~~,~~

~~including the independent organization that will administer the guidelines,~~ if the ~~applicant~~ independent organization demonstrates that the proposed guidelines—

(I) meet or exceed the particular requirements of this title they are intended to address, as identified in the application;

(II) provide for regular review and certification ~~validation~~ by ~~an~~ the independent organization that the activities of the entity or entities falling within the scope of the guidelines ~~to ensure that the covered entity or covered entities adhering to the guidelines~~ continue to meet or exceed the particular requirements of this title they are intended to address; and

(III) include a means of enforcement ~~if~~ where an independent organization determines that an ~~covered~~ entity certified pursuant to the guidelines fails to comply with the ~~does not meet or exceed the requirements in the~~ guidelines, which may include referral to the Commission for enforcement consistent with section 117 or referral to the appropriate State attorney general for enforcement consistent with section 118.

(iii) TIMELINE.—Not later than ~~1 year~~6 months after the date on which the Commission receives an application regarding proposed guidelines pursuant to paragraph (1), the Commission shall issue a determination approving or denying the independent organization's application~~, including the relevant independent organization,~~ and providing the reasons for approving or denying the application.

(B) APPROVAL OF MODIFICATIONS.—

(i) IN GENERAL.—If the independent organization administering a set of guidelines approved under subparagraph (A) makes material changes to the guidelines, the independent organization shall submit the updated guidelines to the Commission for approval. As soon as feasible, the Commission shall publish the updated guidelines and provide an opportunity for public comment.

(ii) TIMELINE.—The Commission shall approve or deny any material change to guidelines submitted under clause (i) not later than ~~1 year~~ 6 months after the date on which the Commission receives the submission for approval.

(b) WITHDRAWAL OF APPROVAL.—

(1) IN GENERAL.—If at any time the Commission determines that guidelines previously approved under this section no longer meet the requirements of this title or that compliance with the approved guidelines is insufficiently enforced by the independent organization administering the guidelines, the Commission shall notify the relevant ~~covered~~ entity or group of ~~covered~~ entities and the independent

organization of the determination of the Commission to withdraw approval of the guidelines, including the basis for the determination.

(2) OPPORTUNITY TO CURE.—

(A) IN GENERAL.—Not later than 180 days after receipt of a notice under paragraph (1), the ~~covered~~ entity or group of ~~covered~~ entities and the independent organization may cure any alleged deficiency with the guidelines or the enforcement of the guidelines and submit each proposed cure to the Commission.

(B) EFFECT ON WITHDRAWAL OF APPROVAL.—If the Commission determines that cures proposed under subparagraph (A) eliminate alleged deficiencies in the guidelines, the Commission may not withdraw the approval of such guidelines on the basis of such deficiencies.

(c) CERTIFICATION AND ATTESTATION.—A covered entity, large data holder, data broker, or service provider ~~with~~ that has been assessed by an independent organization against guidelines approved by the Commission under this section and whose compliance with such guidelines has been certified by the independent organization shall—

(1) publicly ~~self-certify~~ attest that ~~the covered entity~~ it is in compliance with the guidelines; and

(2) as part of the ~~self-certification~~ attestation under paragraph (1), indicate the independent organization responsible for assessing compliance with the guidelines.

(d) REBUTTABLE PRESUMPTION OF COMPLIANCE.—

An ~~covered~~ entity that has been certified by an independent organization as being in compliance with ~~is eligible to participate in~~ guidelines approved under this section~~, participates in the guidelines, and is in compliance with the guidelines~~ shall be entitled to a rebuttable presumption that the ~~covered~~ entity is in compliance with the relevant provisions of this title to which the guidelines apply.