DIGITAL CONSUMER PROTECTION COMMISSION ACT

The *Digital Consumer Protection Commission Act* establishes a new federal commission to regulate digital platforms, including with respect to transparency, competition, privacy, consumer protection, and national security, and to license dominant digital platforms.

Title-by-Title Summary

- **Title I: Establishment of Digital Consumer Protection Commission**. Creates the Digital Consumer Protection Commission, an independent, bipartisan regulator, to promote competition, protect privacy, protect consumers, and strengthen national security with regard to tech platforms. The Commission has investigative, enforcement, and rulemaking authority. "Dominant platforms," defined by factors such as revenue and user base, are subject to more stringent standards.

- **Title II: Transparency Reform.** Requires dominant platforms to disclose terms of service and content moderation criteria and establish prompt user-friendly appeals processes. Dominant platforms must also provide timely notices and appeal options when restricting user access to content or failing to remove or block prohibited material such as CSAM in violation of their terms of service. Users can submit complaints regarding appeal violations of terms of service to the Commission.

- **Title III: Competition Reform.** Prohibits dominant platforms from abuses or attempted abuses of dominance to harm competition. Defines several presumptive abuses of dominance, such as self-preferencing and tying arrangements. Provides for prospective and retrospective merger review, and authorizes including blocking certain mergers/acquisitions and allowing for the breaking up/divestiture of existing monopolies.

- **Title IV: Privacy Reform.** Guarantees several privacy protections, and creates duties of loyalty, care, and mitigation of risks including risks of self-harm, addictive behaviors, physical harm, discrimination, online bullying, harassment, and predatory, unfair or deceptive marketing practices.

- **Title V: National Security Reform.** Limits foreign ownership and access to data of dominant digital platforms, particularly by foreign adversaries.

- **Title VI: Licenses for Operators of Dominant Platforms.** Requires dominant platforms to be licensed and allows license revocation for repeated and egregious violations of the act, including anti-competitive and anti-consumer conduct.

- **Title VII: Enforcement.** Provides for federal, state, and private rights of action to enforce the act.

- **Title VIII: Miscellaneous.** Concerns funding and other issues.

Section-by-Section Summary

Section 1. Short title.

TITLE I – AMENDMENTS TO CLAYTON ACT

Sec. 101. Establishment of Digital Competition Protection Commission. Amends the Clayton Act by designating existing provisions of the Clayton Act as "Division A" and creating a new "Division B" concerning the Commission.

Within that Division B:

Sec. 2001. Table of Contents.

Sec. 2002. Definitions. *[excerpts of key definitions]*

- **Algorithm** – computational process derived from machine learning, statistics, or other data processing or artificial intelligence techniques.
- **Business User** – a person that uses a platform for the sale of goods or services.
- **Child** – person under 18.
- **Control** – includes holding 25% or more equity in a platform or substantial ability to influence.
- **Covered Entity** – any person that collects, processes, or transfers personal data, but excludes government entities, government service providers, and designated nonprofit entities related to missing and exploited children.
- **Critical Trading Partner** – an entity with the power to restrict a business user's access to its own users/customers or essential tools/services.
- **Data Broker** – a person that collects, buys, licenses, or infers data about individuals and then sells, licenses, or trades that data in a commercial transaction.
- **Data Processing** – any operation or set of operations, automated or not, involving personal data, including collection, recording, storage, alternation, retrieval, use, disclosure, dissemination, erasure, or destruction, and includes the sale of personal data.
- **De-Identified Data** – information derived from sensitive personal data that is not reasonably linkable or able to reveal information about an identified or identifiable individual, household, or associated device.
- **Dominant Platform** – as defined in Sec. 2121, a platform that meets certain requirements based on ownership and control, user count, critical trading partnerships, market capitalization, net annual sales, or assets and earnings.
- **Operator** – person who owns or controls a platform.
- **Personal Data** – information collected by a platform identifying or reasonably linkable to a user, individual, or associated device, excluding de-identified data and publicly available information.

- **Platform** – digital service like a website, app, operating system, or digital assistant that allows users to generate or interact with content, facilitates transactions, or enables extensive searches.
- **Platform Conflict of Interest** – conflict that arises when a person owning or controlling a platform also owns or controls a competing business on that platform, allowing them to favor their own business over competitors or disadvantage third-party competitors. It also includes representing both buyers and sellers on the platform.
- **Restricted Country** – country for which a prohibition or policy of denial applies under 22 CFR 126.1.
- **Sensitive Personal Data** – includes various forms of personal information, such as government-issued identifiers, dates of birth, cellphone numbers, health-related data, financial account numbers, credit scores, biometric information, geolocation information, private communications, online activity data, biometric information, persistent identifiers, and other categories designated by the Commission.
- **Terms of Service** – all terms of use, community standards, confidentiality provisions, and other agreements made between the platform user and the platform.

Title I – Establishment of Digital Consumer Protection Commission

Subtitle A—Commission Structure, Jurisdiction, and Powers

- **Sec. 2111. Establishment.** Establishes the Digital Consumer Protection Commission.
- **Sec. 2112. Commissioners.** The Commission consists of 5 Presidentially-appointed commissioners serving 5-year terms, with staggered terms, and subject to qualifications including political party limits and conflict of interest restrictions on financial involvement with platform operators or related entities.
- **Sec. 2113. Designation of Acting Chairperson; sessions; seal.** The Commission's chairperson can designate an acting chairperson in the chairperson's absence, three members constitute a quorum, decisions are made by a majority vote.
- **Sec. 2114. Commission Jurisdiction.** The Commission implements and enforces the Act's provisions, promotes competition, privacy, national security, and transparency on platforms, and has jurisdiction and oversight over all covered entities, including platform operators, and their employees suspected of violating the Act or having knowledge of violations.
- **Sec. 2115. Commission Powers.** The Commission may investigate to identify violations, aid in enforcement, prescribe rules, or recommend legislation. The Commission may conduct administrative enforcement proceedings resulting in, among other outcomes, injunction, civil penalty, disgorgement, and debarment. Parties may apply for rehearing and seek judicial review. The Commission may refer evidence for criminal proceedings, and also has independent litigation authority and the ability to monitor compliance. The Commission has a duty to report at least yearly to Congress.
- **Sec. 2116. Rulemaking Authority.** The Commission may promulgate rules in accordance with 5 U.S.C. § 553 (Administrative Procedure Act).

- **Sec. 2117. Advisory Boards.** The Commission may establish advisory boards for recommendations on particular subjects. The boards must contain academics, platform representatives, public interest advocates, and technical experts. Board members are selected by consensus or in proportion to the political parties of the Commissioners.
- **Sec. 2118. Complaints.** The Commission shall establish a complaint process for public allegations of violations, managed by the Director of the Office of Licensing for Dominant Platforms. The Director will establish a unit for centralized collection, monitoring, and response to complaints, and coordinate with other agencies. Complaints may be made publicly available while protecting personally identifiable information.

Subtitle B– Dominant Platforms

- **Sec. 2121. Dominant Platforms Defined.** Defines dominant platforms (see "Sec. 2002. Definitions"). The Commission must publish designations of dominant platforms. Platforms may submit requests for removal of designations and the Commission's decisions are subject to judicial review. Intentional avoidance of designation is unlawful.

Title II – Transparency Reform

- **Sec. 2201. Transparency Practices and Appeal Rights.** Dominant platform operators must disclose terms of service and content moderation criteria, establish prompt user-friendly appeals processes, and provide timely notices and appeal options when restricting user access to content or failing to remove or block prohibited material in violation of terms of service which may include child sexual abuse materials, cyberbullying, and other harmful content. Exceptions to the notice requirement include cases of imminent harm, terrorism or criminal activity, and law enforcement requests with justification. Users of dominant platforms may submit complaints regarding violations of terms of service to the Commission. Platforms must keep records of complaints and appeals and regularly report to the Commission.
- **Sec. 2202. Best Practices.** The Commission shall establish recommended, standardized content moderation and appeal policies which dominant platforms can adopt.

Title III – Competition Reform

Subtitle A–Antitrust Review

- **Sec. 2311. Abuses of Dominance.** Prohibits dominant platforms from abuse or attempted abuse of dominance to harm competition, or to otherwise harm competition. Defines presumptive abuses of dominance including self-preferencing, tying, noncompete agreements, and predispute arbitration agreement. Gives the Commission authority to define additional abuses of dominance.
- **Sec. 2312. Platform Conflicts of Interest.** Prohibits dominant platform operators from maintaining or creating a platform conflict of interest. The Commission or a court may order the operator to eliminate the conflict by implementing divestitures or other necessary actions. The Commission has the authority to establish rules for defining critical trading partners, enforcing the prohibition, and implementing remedies.
- **Sec. 2313. Future Acquisitions.** Dominant platform operators must file merger notifications under the Clayton Act with both the Commission and the relevant antitrust authority.

Dominant platform operators cannot acquire other entities without demonstrating that the acquisition serves the public interest.

- **Sec. 2314**. **Retrospective Reviews.** The Commission can retrospectively review acquisitions made by dominant platform operators or those resulting in dominant platforms, and if the review determines significant harm to the public interest, the Commission may order remedies such as unwinding the acquisition or requiring divestitures.
- **Sec. 2315. Additional Remedies.** The Commission may investigate any platform operator for violations and can order remedies, including divestitures, to restore competition.
- **Sec. 2316**. **Contractual Transparency.** The Commission may require operators of dominant platforms to disclose contractual terms, including pricing requirements for business users.
- **Sec. 2317. Prohibition on Abusive Acts or Practices.** The Commission may prohibit abusive acts or practices by covered entities that interfere with a user's understanding of the terms of agreement or that take unreasonable advantage of the user's lack of understanding of the platform or inability to protect the user's interests.
- **Sec. 2318. Data Brokers.** An operator of a dominant platform may not sell to a data broker personal data, except in accordance with other laws permitting disclosure of personal data and rules promulgated by the Commission.

Subtitle B– Data Portability and Interoperability

- **Sec. 2321 Data Portability and Interoperability.** The operator of a dominant platform must provide transparent and accessible interfaces to users and authorized third parties for data portability, and to business users and authorized third parties for interoperability. This requirement will not prohibit an operator of a dominant platform from taking indispensable system integrity or data protection measures.

Subtitle C– Miscellaneous

- **Sec. 2331. Rules of Construction.** The act does not alter liability under the antitrust laws or the Federal Trade Commission Act.

Title IV – Privacy Reform

Subtitle A– Covered Entity Duties and Requirements

- **Sec. 2411. Duty of Loyalty.** A covered entity cannot process personal data or design technologies that substantially conflict with a person's best interests with respect to their platform experience or personal data.
- **Sec. 2412. Duty of Care.** A covered entity cannot design or use services or algorithms, or process personal data in a way that causes or is likely to cause physical, economic, relational, reputational, or psychological harm, discrimination, or significant adverse effects. Exceptions include self-testing to prevent discrimination, diversifying pools, and providing resources for harm prevention. Excludes from coverage private clubs or groups not open to the public.
- **Sec. 2413. Duty of Mitigation.** Covered entities must mitigate risks of physical, emotional, developmental, or material harms posed by platforms controlled by the covered entity, including self-harm, addictive behaviors, physical harm, online bullying, harassment, and

predatory, unfair or deceptive marketing practices. Covered entities must establish safeguards to control personal data, including settings allowing users to restrict others' access to their personal data, limit features that extend use of the platform, opt out of algorithmic recommendation systems, delete user accounts or data upon request, restrict sharing of geolocation information, and limit time spent on the platform. The default settings of a platform must be set at the most protective settings.

- **Sec. 2414. Duty of Confidentiality; Data Collection and Processing.** A covered entity may process personal data only if it is necessary for contract performance, legal compliance, protection of vital interests, performance of a public task, or pursuit of legitimate interests. A covered entity must ensure that processing of personal data is limited to what is necessary for the articulated purpose.
- **Sec. 2415. Limitations on Targeted Advertising.** A covered platform operator cannot target advertising to a user based on personal data from other platforms, except for the user's first-party data or in response to their request.
- **Sec. 2416. Rights of Data Subjects to Access, Correction, Portability, and Deletion.** A person has the right to access all personal data processed by a covered entity. A person also has the right to access all information regarding the collection and processing of their personal data, including where the data was obtained, to whom it was disclosed, the purpose of the processing, and the period of retention. A person also has the right to obtain, correct, delete, and request the cessation of collection and use of their personal data processed by a covered entity, and to obtain the data in a format suitable for use and transmission in a machine-readable format, as well as a means to exercise these rights without additional cost or penalty. The Commission will establish compliance deadlines for these requests.
- **Sec. 2417. Right to Know.** A person has the right to know what personal data a covered entity will collect and process before giving consent. Covered entities must make publicly available privacy policies, with requirements to be specified by the Commission.

Subtitle B–Data Security Reform

- **Sec. 2421. Data Security Safeguards.** A covered entity must safeguard personal data through reasonable security measures and maintain a comprehensive information security program that protects against unauthorized access or loss, including documenting, assessing, designing, implementing, testing, and modifying safeguards as needed.
- **Sec. 2422. Civil Penalties and Damages For Data Breaches.** The Commission can order a covered entity to pay a civil penalty of $150 per breach of personal data, with $50 of the penalty amount being paid to the affected person, not exceeding 50% of the parent entity's revenue. Failure to notify the Commission or affected person within 30 days of a data breach may result in doubling the penalty, not exceeding 75% of the parent entity's revenue. Compliance with Sec. 2421 exempts a covered entity from penalties. In a civil action brought by a person who is affected by a data breach, damages may be $100 per breach or actual damages, whichever is greater.

Subtitle C– Miscellaneous

- **Sec. 2431. Authority to Propose and Establish Heightened Requirements For Dominant Platform Operators.** An Advisory Board may propose heightened requirements for operators of dominant platforms, and the Commission may promulgate rules to do the same.

Title V – National Security Reform

- **Sec. 2501. Corporate Citizenship and Ownership.** Defines "foreign adversary" with reference to the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1607(c)). An operator of a dominant platform must be a citizen of the U.S. or own a subsidiary corporation that is a citizen of the United States and that has less than half of its directors as noncitizens. No director of such a subsidiary may be a citizen of a foreign adversary. If over 10% of a dominant platform operator's owners are citizens of a foreign adversary, the operator must sequester back-end data, algorithms, and information related to U.S. users, preventing access by any subsidiary, affiliate, director, employee, or agent based outside of the U.S. The Committee on Foreign Investment in the United States must treat the application of a foreign person for a license as a covered transaction, and if the Committee determines the provision of a license threatens to impair national security, the Commission shall deny the application for the license.
- **Sec. 2502. Limitation of Data Processing in Restricted Countries.** An operator of a dominant platform may not process the personal data of a U.S. person in a restricted country.
- **Sec. 2503. Bot and Country of Origin Identifications.** An operator of a dominant platform must publicly identify any post generated by a non-human user, as well as the country of origin of the post. The identification must accompany the post anywhere it appears on the platform.

Title VI – Licenses for Operators of Dominant Platforms

- **Sec. 2601. Licensing Office.** The Office of Licensing for Dominant Platforms is established within the Commission, headed by a Director appointed by the President for a 4-year term, responsible for reviewing and granting licenses for dominant platforms, monitoring compliance, managing complaints, and referring violations for enforcement, with the authority to rescind or revoke licenses when necessary.
- **Sec. 2602. Requirement for Operators of Dominant Platforms to Obtain Licenses.** The Office grants licenses to designated dominant platform operators, and failure to obtain a license prohibits the operator from operating as a legal entity under federal law, with licenses subject to rescission if the platform's dominant status is removed.
- **Sec. 2603. Revocation of License.** Sets forth the grounds and procedures for license revocation, which is subject to judicial review.
- **Sec. 2604. Compliance Certification.** Dominant platform executives must annually certify compliance with Titles II, III, IV, and V of the act, and are subject to civil and criminal penalties for knowingly false statements.

Title VII – Enforcement by Other Entities

- **Sec. 2701. Enforcement by States, Private Parties, and Federal Agencies.** Provides for enforcement by state attorneys general and allows private rights of action by injured parties. Provides for enforcement by FTC for violations of Titles III and IV, and enforcement by DOJ for violations of Title III. Sets forth factors to consider in awarding punitive damages.
- **Sec. 2702. Exclusive Jurisdiction.** Federal courts have exclusive jurisdiction. All appeals of Commission decisions must be brought in the Court of Appeals for the D.C. Circuit. The U.S. District Court for the District of Columbia has exclusive jurisdiction over constitutional challenges to the Act.

Title VIII – Miscellaneous

- **Sec. 2801. Funding.** $500,000,000 for FY 2023 and each year thereafter. The Commission may use amounts collected under the Act to carry out its functions.
- **Sec. 2802. Interagency Cooperation.** The Commission must coordinate with DOJ and the FTC.
- **Sec. 2803. Effective Date.** One year after enactment of the Act, except as provided otherwise.
- **Sec. 2804. Rules of Construction.** No preemption of state law if it offers greater protection to users and consumers . No limiting of FTC, DOJ, or any other federal agency jurisdiction.
- **Sec. 2805. Severability.** If one provision of the act is invalidated, the remainder of the act is protected.

TITLE II – AMENDMENTS TO OTHER LAWS

Sec. 201. Executive Accountability for Operators of Dominant Platforms. Creates criminal liability for executives of dominant platforms who negligently allow certain violations of the law.

Sec. 202. Criminal Fines Under the Sherman Act. Changes the maximum penalties under the Sherman Act.

Sec. 203. Criminal Fines Under the Robinson-Patman Act. Changes the maximum penalty under the Robinson-Patman Act.

Sec. 204. Directing the Attorney General to Develop Victim-Centered Guidance. Directs the Attorney General to establish protections and assistance for child sex trafficking victims who testify against human traffickers. Provides for training concerning victim-centered protocols for DOJ, prosecutors and judges, enhanced victim restitution procedures, and technical changes to certain block grants concerning child human trafficking.

Sec. 205. Use of the term “Child Sexual Abuse Material.”Amends several federal statutes to replace the term “child pornography” with the term “child sexual abuse material.”

Sec. 205. Ineligibility due to disqualifying mental status. Amends several federal statutes to replace the term “adjudicated as a mental defective” with the term “adjudicated as ineligible due to disqualifying mental status.”