Data Transfer Initiative

Table 1. Legislation in the United States and Europe

Essential provisions	**General Data Protection Regulation (2016)**	**Digital Markets Act (2022)**	**ACCESS Act (2022) [proposed]**	**Digital Consumer Protection Commission Act (2023) [proposed]**	**New York Senate Bill 6686 (2023) [proposed]**
Approach to data sharing	Data subjects have the right to receive the personal data they have provided to a controller in a "structured, commonly used, and machine-readable" format (Article 20.1). Users also have the right to have their personal data transmitted directly between controllers (Article 20.2).	Gatekeepers must ensure "real-time and continuous" portability for users and authorized third parties (Article 6.9). They must also provide business users functionally equivalent access to features of core platform services (Article 6.7). Messaging services must become interoperable (Article 7).	Large communications platform providers ("platform providers") have "general duties" to maintain interfaces that enable data portability and interoperability (§3-4). These duties require platform providers to give competing services access to their interfaces on terms that are fair, reasonable, and nondiscriminatory (§4).	Dominant platforms must create tools that allow users and authorized third parties to transfer their data. They must also provide business users with functionally equivalent access to features and "continuous and real-time" access to user data (§2321). In addition, users have the right to download their personal data and transfer it to another service (§2416).	Social media companies must provide an Application Programming Interface (API) that allows users and "Authorized Representatives" access to their personal data (§1101).
Technical requirements	Data controllers	Gatekeepers must	Platform providers	Dominant platforms	Social media companies

	possess significant latitude as to how they transfer personal data, including the format and means of transfer, which must only be "technically feasible" (Article 20.2).	develop "tools" for guaranteeing data portability (Article 6.9). Messaging services must provide technical interfaces (or similar solutions) for facilitating interoperability (Article 7.1).	must expose distinct interfaces for data portability and interoperability (§3-4). Platform providers possess some autonomy in the design of these interfaces (§4), though changes must be publicly announced (§4).	must expose interfaces for data portability (§2321). They must also provide business users with "tools" to access the dominant platform's data (§2321).	must open an API that permits third parties to retrieve data and send instructions on behalf of users and Authorized Representatives for fair, reasonable, and nondiscriminatory prices (§1101).
Documentation requirements			Platform providers must produce "complete and accurate" documentation for the interoperability interface (§4). Documentation must describe how to access the interface and disclose all information "necessary" for development of interoperable products (§4).		Social media companies must provide documentation that contains all information "reasonably necessary" to access the API (§1101). Documentation must specifically include API syntax, instructions for interacting with the API, technical requirements for registering applications, and change logs (§1101).
Applicability	Applies to data	Applies to the specific	Applies to platform	Applies to "dominant	Applies to all social

	"controllers" and "processors." Controllers are entities that determine the purpose and means of processing personal data (Article 4.7). Processors are entities which process personal data on behalf of a specific controller (Article 4.8).	"core platform services" of "gatekeepers." Core platform services are one of a variety of digital services that connect business users with end users (Article 2.2). Gatekeepers are digital services that have high market capitalization (>EUR 75 billion) and numbers of end users (>45 million) (Article 3.1-3.2). Gatekeepers are designated by the European Commission (Article 3).	providers that control services which generate income by processing data and have more than 100,000,000 monthly active users in the US (§2).	platforms" and/or "covered entities." Dominant platforms are publicly traded and have greater than 50,000,000 users and 100,000 business users *and* one of the following: $550 billion in revenue, $550 billion in market capitalization, or 1 billion users worldwide (§2121). Dominant platforms are designated by the new Digital Consumer Protection Commission (§2121). Covered entities are persons that collect and process personal data (§2002).	media companies regardless of size (§1100). Social media platforms are services that allow users to interact socially within an application and, specifically, create profiles, follow other users, and share content (§1100).
Scope of data	The scope of data includes all "personal" data. Personal data is any information relating to an identified or identifiable natural	For data portability, the scope of data includes data that is "provided" by users or "generated" by a gatekeeper based on provided data (Article	The scope of data includes any information that is "collected directly" by the platform provider and "reasonably linkable" to a person	The scope of data includes data that is "provided" by users or "generated" based on user activity (§2321). The right to data portability includes all	The scope of data includes data that is "controlled" by the social media company (provided, inferred, and interaction data) as well as content (§1101)

	person (Article 4.1).	6.9).	(§1). Anonymized data is not included (§1).	personal data that has been processed (§2416).	
Third-party access	Data subjects can request that their personal data be transferred to third-party controllers (Article 20.2).	For data portability, users can authorize third parties to receive data from gatekeepers (Article 6.9).	"Custodial third-party agents" are entities authorized by users to manage their data (§1). Platforms must maintain specific interfaces for third-party agents (§5). Third-party agents have a duty to protect user data and act in the best interests of users (§5).	Users and business users can authorize third parties to receive data from dominant platforms (§2321). The right to data portability allows users to request that covered entities transfer personal data to other covered entities (§2416).	"Authorized Representatives" are entities that users have authorized to take actions on the social media platform (§1100). "Third-party applications" are another group that have access, but it is unclear how this group is different from Authorized Representatives.
Reciprocity		Gatekeepers may not collect and process the personal data of end users received from third-party services without consent or another legal basis (Article 5.2). Gatekeepers must also minimize data collected from messaging services that	Platform providers may not collect or use data shared with them by competing services except to safeguard privacy and maintain interoperability (§4). They also may not use shared data for commercial purposes (§4).	All platforms (regardless of their designation) cannot target advertising towards users with data received from third parties (§2415).	

		interoperate with their core platform services (Article 7.8).			
Access controls		Gatekeepers must publish general access conditions for their app stores, search engines, and social media platforms (Article 6.12). Terms must be fair, reasonable, and non-discriminatory. Terms for restricting access cannot be disproportionate (Article 6.13).	Platform providers can set reasonable thresholds for API usage, expectations for governance, and fees for API access (§4). Platform providers can also revoke third-party agents' access if they repeatedly abuse API access (§5). Platform providers cannot unreasonably deny access to APIs (§4).	Dominant platforms can take "indispensable" and "duly justified" measures to prevent data portability and interoperability from compromising the privacy, security, and integrity of systems (§2321). This presumably includes conditions for denial of access.	Social media companies can restrict access to APIs if Authorized Representatives engage in abusive behavior (§1100). Social media companies must maintain records of when they choose to deny API access (§1102).
Privacy and security	The right to data portability may not "adversely affect the rights and freedoms of others" (Article 20.4). In addition, controllers' data processing must comply with several general principles (Article 5), possess a legal basis (Article 6),	While gatekeepers must ensure interoperability, they can still take measures to protect the security and integrity of their services (Articles 6.4, 6.7, 7.3 & 7.8). Such measures must be "strictly necessary and proportionate" as well as "duly justified" by	Platform providers must set minimum security standards for third-party access to user data (§4). Competing services and third-party agents also possess duties to protect the security of user data (§5).	In addition to the above, covered entities possess a variety of duties that govern how they can process personal data (§2411-2414). Covered entities must set safeguards for data security (§2421).	Social media companies are required to conduct assessments that APIs successfully implement privacy and security features (§1102).

	and undergo a variety of procedural protections (e.g., Article 35).	gatekeepers (Articles 6.4 & 6.7).			
Standards Development		The European Commission may mandate that European standards bodies develop standards (Article 48).	The National Institute for Standards and Technology is charged with developing standards for interoperability of online messaging, multimedia sharing, and social networking (§6). These standards act as safe harbors (§6).	The new Commission must set standards for best practices in content moderation (§2202) and short-form privacy policies (§2417).	

Enforcement and Implementation	"Supervisory authorities" within each EU member state lead enforcement. Supervisory authorities are designated by each member state and must be completely independent (Articles 51-52). Supervisory authorities possess a variety of investigative and corrective powers to conduct their enforcement (Article 58).	The European Commission spearheads enforcement and implementation. It can adopt and suspend "implementing acts" to ensure gatekeepers comply with their obligations (Articles 8.2 & 9.1). The Commission can also issue "delegated acts" to amend elements of the law (Article 12).	The FTC is charged with enforcement. It regularly assesses compliance and hears complaints from users and third-party agents (§6). The FTC possesses the same enforcement powers as under the FTC Act and can levy fines (§6).	A new "Digital Consumer Protection Commission" is charged with enforcement. Similar in structure to the FTC, the Commission's jurisdiction extends to promoting competition, privacy, national security, and transparency on platforms (§2114). It has a variety of powers to investigate and issue orders (§2115).	The New York Attorney General is charged with enforcement. Social media companies must conduct routine tests to ensure the API complies with technical requirements (§1102). They must submit an API access report that includes information about features and denials of access (§1102).