CENTER FOR DEMOCRACY & TECHNOLOGY

Independent Researcher Access to Social Media Data: Comparing Legislative Proposals

Researchers use data from social media companies and other hosts of user-generated content to study important topics of public concern, such as the efficacy of different content moderation efforts and ideas to improve them, the spread of dis- and mis-information online, ranking and recommendation algorithms, and online advertising. But some researchers have been stymied by the type and amount of data available, the level of control that social media companies exert over researchers' access, and other barriers.

Lawmakers in both the United States and Europe are increasingly focused on how to meet the needs of independent researchers who want better access to data from social media companies to conduct research in the public interest, while at the same time balancing user privacy and other concerns.

In the last year, members of the US Congress have introduced or published at least four bills or discussion drafts with provisions about researcher access to data held by online services: The Platform Accountability and Transparency Act, Social Media Data Act, Digital Services Oversight and Safety Act, and Kids Online Safety Act.

In Europe, Article 31 of the Digital Services Act will become the first major legislation requiring some online services to make certain data available to researchers. In July 2022, the European Parliament adopted the DSA. The provisions of Article 31 are expected to go into effect in late 2022 or early 2023.

In addition to proposals *requiring* social media companies to disclose data to researchers, lawmakers and others are also considering how best to *permit* these companies to disclose data to researchers voluntarily and consistent with privacy laws. The European Digital Media Observatory has published a report and draft Code of Conduct pursuant to Article 40 of the General Data Protection Regulation to provide guidance on how technology companies can voluntarily share data with researchers in compliance with the GDPR. In the United States, Section 101(b) of the American Data Privacy and Protection Act would allow for the collecting, processing, or transferring covered data for research projects that meet certain criteria

CDT has compiled a chart (last updated on July 8, 2022) comparing how these different researcher access to data proposals answer seven key questions.

Table of Contents

I. Who would have access to data?

Platform Accountability and Transparency Act	"Qualified researchers" = "a **university-affiliated researcher** specifically identified in a research proposal that is approved by the NSF to conduct research as a qualified research project" (Sec. 2) **Public access to some data:** Gives the FTC rulemaking authority to require covered platforms to report certain other data or information to **the public,** qualified researchers, or some combination of the two (Sec. 12(a)) and requires the FTC to issue rules requiring platforms to make **public reports** about **content that has been highly disseminated** (Sec. 12(b)), **advertising** (Sec. 12(c)), **algorithms** (Sec. 12(d)), and **content moderation** (Sec. 12(e)).
Social Media Data Act	**Academic researchers** and the **FTC**. (Sec. 2(a)(1)) Academic researcher = an individual that conducts research in collaboration with an **institution of higher education** (as defined in section 6 101(a) of the Higher Education Act of 1965) and research is not for commercial purposes. (FTC may update definition as needed) (Sec. 2(d)(1))
Digital Services Oversight and Safety Act	**Researchers affiliated with an institution of higher education** or **nonprofit** whose mission includes developing a deeper understanding of the impacts of platforms on society.

	Both organizations and researchers must be certified by the Office of Independent Research Facilitation to be established at the FTC. "**Host organizations**" must meet requirements TBD by the FTC and commit to training researchers, reviewing research projects, and other commitments. "**Certified researchers**" must meet requirements established by the FTC and make commitments, such as compliance with information or security requirements established by the FTC, agreeing not to attempt to reidentify data, agreeing to publish their research, and more. (Sec. 10(b)) **Public access to some data**: Requires FTC to issue regulations requiring a provider of a hosting service to issue **publicly available transparency reports** relating to content moderation. (Sec. 6(b)) Requires FTC to issue regulations requiring providers of a large covered platform to maintain a public version of an **advertising library** (Sec. 10(f), 10(f)(3)) and a public version of a **high-reach public content stream** (Sec. 10(g), 10(g)(4)).
Kids Online Safety Act	"Qualified researchers" = (1) Affiliated with an **institution of higher education** or a **nonprofit organization**, including any 501(c); *and* (2) **Approved** by Assistant Secretary of Commerce for Communications and Information (NTIA) To gain approval, a researcher must: Conduct the research for **noncommercial purposes**; Demonstrate a **proven record of expertise** on the research topic and related research methodologies; and Commit to fulfill, and demonstrate a capacity to fulfill, specific **data security and confidentiality requirements** corresponding to the application. (Sec. 7(a)(2), 7(a)(5), (b))
DSA Art. 31	**Vetted researchers** who meet certain conditions: (a) **Affiliation with research organisations** as defined in Article 2, point 1, of Directive (EU) 2019/790 [Under Article 2, point 1 of Directive (EU) 2019/790, **"research organisation"** = a **university**, including its libraries, a **research institute** or **any other entity**, the **primary goal of which is to conduct scientific research** or to carry out educational activities involving also the conduct of scientific research on a **not-for-profit basis** or by reinvesting all the profits in its scientific research; or pursuant to a **public interest**

	mission recognised by a Member State. Research must be carried out in such a way that "the access to the results generated by such scientific research cannot be enjoyed on a preferential basis by an undertaking that exercises a decisive influence upon such organisation."] (b) **Independence from commercial interests** (ba) **Must disclose the funding of their research** (c) Capable of preserving **specific data security and confidentiality requirements** (and request must describe the technical and organisational measures put in place to this end) (d) Submission of an application justifying the **necessity and proportionality** of the data requested for research, the timeframe for data access, and the contribution of the expected research results to the purpose for which access may be granted (e) Limited to research activities of purposes set forth in Art. 31, para. 2 [See Section III in this chart] (f) Commit to making their research **publicly available free of charge** (Art. 31 para. 2 & 4) **Access to some public data by other researchers**: Researchers, including those affiliated with non-profits who meet some of the vetting criteria of Art. 31 para. 4 (subparts (a), (b), (ba), (c), and (d)) will be given access to data that is "publicly accessible in [a very large online platforms'] online interface for researchers." (Art. 31 para. 4d)
EDMO Draft Code of Conduct	Any researcher conducting **"qualifying research."** Factors to consider in determining whether research is "qualifying research": The **purpose** of the research should be to **develop society's collective knowledge** and should be primarily **noncommercial**. The **entity carrying out the research** should have as one of its principal aims the conduct of research on a **not-for-profit basis** pursuant to a **state-recognised public-interest mission. Access to the results** of the research should **not be enjoyed on a preferential basis** by any entity that exercises a decisive influence on the organisation. The entity must be **able to explain** its **decision-making processes** and **funding**

	structure. It must **not perform law enforcement, intelligence services, or defence/national security functions** and must be independent from any public body carrying out those functions. **Field of inquiry** is interpreted broadly [See Section III of this Chart]. The research must comply with **specified methodological and ethical standards**. There must be a **specific research project** with **specific research objectives**. (Preamble para. 12-16)
American Data Privacy and Protection Act	Any public or peer-reviewed scientific, historical, or statistical research project that otherwise meets the requirements of the permissible purpose. [See Sections III, V, and VI of this Chart] (Sec. 101(b)(9))

CENTER FOR DEMOCRACY & TECHNOLOGY

II. What types of data would be accessible to "researchers," specifically?

Platform Accountability and Transparency Act	"Qualified data and information" = "data and information from a platform that the NSF determines is necessary to allow a qualified researcher to carry out the research contemplated under a **qualified research project**." (Sec. 2). The criteria for "qualified data and information" is **TBD** by the NSF, but it must at least be (1) **feasible** for the platform to provide; (2) **proportionate** to the needs of the qualified researchers to complete the qualified research project; and (3) not cause the platform **undue burden**. (Sec. 4). Qualified data and information **could include non-public content data and personally identifiable information**.
Social Media Data Act	**Ad library** with certain **specified information about any advertiser** that purchases $500 or more of advertising in a calendar year: name and unique identification number of the advertiser, digital copy of the ad, targeting method & description of target audience, optimization objective chosen by advertiser, description of the actual audience, number of views, ad conversion, date and time of ad display, amount advertiser budgeted and paid, ad category (such as politics, employment opportunity, housing opportunity, or apparel), ad language, and platform's advertising policy. (Sec. 2(a)(1)) Would also establish a **Working Group for Social Media Research Access at the FTC** to study making other data and information available to academic researchers (Sec. 2(c))
Digital Services Oversight and Safety Act	The FTC must issue regs identifying the precise types of information that will be available. The FTC regs can specify any relevant information, but it **must consider** particular information: info about **internal platform studies**; info about **content moderation decisions and policies,** the people setting the policies and making decisions, & the training of moderators; **third party requests** to act on a user, account, or content; **engagement and exposure data**; classification of **information sources**; **archives of removed content and accounts**; **Advertisements** and influencer marketing content; detailed information about a platform's **algorithms**. (Sec. 10(c)).

	The information required to be disclosed by FTC regulations **could include non-public content data and personally identifiable information**, but the FTC must require platforms to **deidentify certain data** (non-public data, personal health information, biometric information, and information related to a person under 13 years old), before it may be disclosed and also restricts sharing of precise location information. (Sec. 10(c)(6)) In addition, the FTC must issue regulations requiring covered platforms to submit a **data dictionary** describing the information that can be provided to certified researchers. (Sec. 10(d)) The FTC must also issue regulations requiring large covered platforms to give researchers and the FTC access to an **ad library** (Sec. 10(f)) and a **"high-reach public content stream."** (Sec. 10(g)).
Kids Online Safety Act	Data assets that can be used to conduct **public interest research regarding harms to the safety and well being of minors**, including the following types of matters: (1) promotion of self-harm, suicide, eating disorders, substance abuse, and other matters that pose a risk to physical and mental health of a minor; (2) patterns of use that indicate or encourage addiction-like behaviors; (3) physical harm, online bullying, and harassment of a minor; (4) sexual exploitation, including enticement, grooming, sex trafficking, and sexual abuse of minors and trafficking of online child sexual abuse material; (5) promotion and marketing of products or services that are unlawful for minors, such as illegal drugs, tobacco, gambling, or alcohol; and (6) predatory, unfair, or deceptive marketing practices. (Sec. 3(b), 7(b)(1)) The term "data assets" is not defined in the statute, and could include **non-public content data and personally identifiable information.**
DSA Art. 31	Any data that serves the **permissible purposes of research** specified in Art. 31 para. 2 [See Section III of this Chart], **unless** the 'very large online platform' **(VLOP) does not have access to the data** or giving access would lead to **significant security vulnerabilities** or reveal **confidential information**, in particular **trade secrets**. (Art. 31 para. 2, 2a)

CENTER FOR DEMOCRACY & TECHNOLOGY

EDMO Draft Code of Conduct	**Personal data** as defined by Article 4(1) GDPR (Preamble para. 19) for which there is a **legal basis for processing** under the GDPR. (Part I, Section 3). "**Special category data**" (as defined by the GDPR) must only be processed "for research in accordance with a valid exemption and with specific measures in place to safeguard the fundamental rights and interests of data subjects." (Part I, Section 3) Note: The Code of Conduct does not require that researchers be given access to data; rather, it establishes a process under which researchers may be given access to "personal data" in compliance with the GDPR. The GDPR does not restrict researchers' access to data that is not "personal data," and researchers may use data that is not "personal data" without restriction.
American Data Privacy and Protection Act	**Covered data** as defined by the bill, as long as the collection, processing, or transfer of data is "**reasonably necessary, proportionate, and limited**" to a public or peer-reviewed scientific, historical, or statistical research project. (Sec. 101(b), Sec. 101(b)(9)) "Covered data" = "information that **identifies or is linked or reasonably linkable to an individual or a device** that identifies or is linked or reasonably linkable to 1 or more individuals, including derived data and unique identifiers." Covered data **does not include de-identified data**; **employee data; publicly available information; or inferences made exclusively from multiple sources of publicly available information that do not reveal sensitive covered data**. (Sec. 2(8)) Note: The American Data Privacy and Protection Act does not require that researchers be given access to data; rather, it restricts what covered entities may do with covered data and includes certain research as a "permissible purpose" of using covered data. Researchers may collect, process, or transfer data that is not "covered data" under the American Data Privacy and Protection Act without restriction.

CENTER FOR DEMOCRACY & TECHNOLOGY

III. Are there restrictions on the purpose of the research or research project?

Platform Accountability and Transparency Act	Only "qualified research projects" approved by NSF. A qualified research project must (1) have **IRB approval** or be exempt or excluded from IRB approval; (2) "**aim to study activity on a platform**"; (3) meet other criteria **TBD** by the NSF. (Sec. 4)
Social Media Data Act	**None**.
Digital Services Oversight and Safety Act	Researchers may be certified to gain access to information only for the purposes specified in the Act: "to gain understanding and measure the **impacts of the content moderation, product design decisions, and algorithms** of covered platforms **on society, politics, the spread of hate, harassment, and extremism, security, privacy, and physical and mental health**." (Sec. 10(b)(1) & (2))
Kids Online Safety Act	Researchers may access data only to conduct **public interest research** pertaining to **harm to the safety and wellbeing of minors.** Public interest research = scientific or historical analysis of information that is performed for the primary purpose of advancing a broadly recognized public interest. (Sec. 7(a)(4), (b)(1))
DSA Art. 31	Data given to vetted researchers may be used only for research that contributes to the **detection, identification, and understanding of specified systemic risks in the European Union** set out in Art. 26(1) and **assessment of mitigation measures** pursuant to Art. 27(1). (Art. 31 para. 2) In addition, the **Commission must adopt delegated acts** laying down, among other things, the purposes for which the data provided to vetted researchers may be used. (Art. 31 para. 5) Data given to other researchers pursuant to Art. 31, para. 4d may be used only for research that contributes to the detection, identification and understanding of systemic risks in the European Union set out in Art. 26(1). (Art. 31 para. 4d)

EDMO Draft Code of Conduct	The Code of Conduct applies "broadly" to research in **natural sciences, social sciences, humanities, computer science, engineering, and other fields**. (Preamble para. 14)
American Data Privacy and Protection Act	Research must be **scientific, historical or statistical research** that is **in the public interest**. (Sec. 101(b)(9), Sec. 209(b)(9)(A)(i))

CENTER FOR DEMOCRACY & TECHNOLOGY

IV. Which online services must make data available?

Platform Accountability and Transparency Act	"Platforms" = Subject to FTC jurisdiction under section 5(a)(2) of FTC Act; and Is a website, desktop application, or mobile application that **allows users to establish accounts to share user-generated content** and whose primary purpose is for users to interact with user-generated content and for the **platform to deliver ads to users**; and has at least **25 million unique monthly users** in the United States for a majority of the months in the most recent 12-month period. (Sec. 2)
Social Media Data Act	"Covered platform" = any website, desktop application, or mobile application that is **consumer-facing**; and **sells digital advertising space**; and has more than **100 million monthly active users** for a majority of months during the preceding 12 months. **FTC can update definition** as needed. (Sec. 2(d)(3))
Digital Services Oversight and Safety Act	"Covered platform" = A hosting service that **stores information provided by, and at the request of, users** and which, **at the request of users, stores and disseminates information to the public**; and has at least **10 million monthly active users**. The methodology for determining MAU will be determined through rulemaking. (Sec. 2(11); Sec. 10(c)) In issuing the regulations about the types of information that must be disclosed, the manner of disclosure, and whether disclosure is mandatory or optional, the FTC must "**vary the specifications based on the size and scope of a covered platform**, including by having different specifications for different services.
Kids Online Safety Act	"Covered platforms" = a commercial software application or electronic

	service that connects to the internet and that **is used, or is reasonably likely to be used, by a minor**. (Sec. 2(2), Sec. 7(b)(3))
DSA Art. 31	Providers of Very Large Online Platforms (VLOP) = platforms which reach a number of **average monthly active recipients of the service** in the EU equal to or higher than **45 million** and are **designated as VLOPs** by the Commission. Number of average monthly active recipients **can be adjusted** based on changes to the EU population. (Art. 25) "Online platforms" = a provider of a hosting service which, at the request of a recipient of the service, **stores and disseminates to the public information**, unless that activity is a minor or a purely ancillary feature of another service or a minor functionality of the principal and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of the DSA. (Art. 2)
EDMO Draft Code of Conduct	The Code of Conduct does not require any service to make data available. It provides guidance on how a data controller may act as a Data Sharing Organisation (DSO) and voluntarily provide personal data to researchers in compliance with the GDPR.
American Data Privacy and Protection Act	The American Data Privacy and Protection Act does not require any service to make data available. It provides an exception for covered entities to collect, process, or transfer data for research purposes. **"Covered entity" =** any entity or person, other than an individual acting in a non-commercial context, that collects, processes, or transfered covered data and **is subject to the FTC Act,** is a **common carrier subject to Title II of the Communications Act, or** is an **organization not organized to carry on business for their own profit or that of their members.** Also "includes any entity or person that controls, is controlled by, or is under common control with another covered entity." (Sec. 2(9))

CENTER FOR DEMOCRACY & TECHNOLOGY

V. What privacy and security safeguards would there be for data made available to researchers?

Platform Accountability and Transparency Act	Newly-established **FTC Platform Accountability and Transparency Office** (Sec. 3) would establish criteria for privacy and cybersecurity safeguards required for qualified data and information related to a qualified research project, and **can require** reasonable privacy and cybersecurity safeguards for particular data sharing, such as **encryption of data**; delivery of **deidentified data**; use and monitoring of a **secure environment** to facilitate delivery of data. (Sec. 4(j))
Social Media Data Act	**None**. The **Working Group for Social Media Research Access** would study privacy preserving techniques for **other data** that could be made accessible to academic researchers. (Sec. 2(c))
Digital Services Oversight and Safety Act	**Tiered access:** More sensitive info has more safeguards and is accessed by fewer researchers than less sensitive info. (Sec. 10(c)(2)) The FTC must issue regulations specifying the manner in which information is to be accessed, including **when privacy protecting techniques** "such as differential privacy and statistical noise" should be used, **what information security standards should be in place**, and other privacy and security measures. (Sec. 10(c)(4)) The FTC must issue regulations specifying when the Commission should **review research before it is published to protect user privacy** or trade secrets. (Sec. 10(c)(5)) FTC regulations must ensure that provision of access to information does not infringe upon reasonable expectations of personal privacy and must **require platforms to deidentify certain information before it can be provided:** nonpublic information, personal health information, biometric information, information about a child under 13 years old. Also restricts sharing of precise location information. (Sec. 10(c)(6)).

	Users who do not post public content must be given the ability to **opt-out** of having their information shared with researchers. (Sec. 10(c)(6)(C))
Kids Online Safety Act	The NTIA must **establish standards for privacy, security, and confidentiality** required to participate in the program for a researcher to receive, and a covered platform to provide, data assets. (Sec. 7(b)(4)(C)) Imposes a **duty of confidentiality** on a qualified researcher with respect to data assets provided by a covered platform. The duty of confidentiality may be defined further by the NTIA. (Sec. 7(b)(5))
DSA Art. 31	A vetted researcher must have the capacity to preserve the **specific data security and confidentiality requirements** for each request for data and to **protect personal data**. A request for data must describe **appropriate technical and organisational measures** put in place for data security, confidentiality, and to protect personal data. (Art. 31 para. 4) **Specific privacy and security safeguards are TBD**: The Commission must adopt **delegated acts** laying down, among other things, the specific conditions and procedures under which sharing of data with researchers can take place in compliance with the GDPR, taking into account the rights and interests of the providers of very large online platforms and the recipients of the service, "including the **protection of confidential information**, in particular **trade secrets**, and maintaining the **security of their service**." (Art. 31 para. 5.)
EDMO Draft Code of Conduct	The Code of Conduct incorporates the GDPR's requirement that data **must be processed securely and** the requirement that **"appropriate technical or organisational measures"** be used in data processing. The particular security measures that will be appropriate will **depend on the nature, scope, context, and purpose** of the processing and the **risks to individuals' rights and freedoms**. DSOs and researchers should perform a **risk assessment using factors in Part II of the Code** to analyse research risks and mitigation measures. Security measures must be incorporated as **binding and enforceable commitments** into data sharing agreements between DSOs and researchers. Only **data necessary to achieve the research objectives** should be processed. (Part I, Section 4) **Part II of the Code of Conduct provides guidance** on the common risks that arise in DSO-to-researcher data sharing (Part II, Section 5), as well as guidance on technical and organisational measures that may be

	appropriate as safeguards, depending on the data being processed and risk assessment. (Part II, Section 6)
American Data Privacy and Protection Act	Research must adhere to **all relevant laws governing such research** and the **regulations for human subject research in 45 C.F.R. § 46**. (Sec. 101(b)(9)(A)(ii), (iii)). The bill contains **no specific privacy or security safeguards** covered entities must follow to qualify for the exception.

CENTER FOR DEMOCRACY & TECHNOLOGY

VI. What would be the method or mechanism for vetting researchers and providing access?

Platform Accountability and Transparency Act	The NSF **vets the researcher and research project** and **determines what data** a platform must make available; the Platform Accountability and Transparency Office informs the platform and **establishes the privacy and cybersecurity safeguards** for the particular data at issue. Step 1: A researcher submits a research application to the NSF Step 2: The NSF determines if it is a "qualified research project" by a "qualified researcher." Step 3: The NSF identifies the "qualified data and information" that platforms will be required to make available to the researcher, and in what form. Step 4: The NSF refers the qualified research project to the FTC Platform Accountability and Transparency Office Step 5: The Office notifies the platform that it will be required to provide data and establishes reasonable privacy and cybersecurity safeguards for the data. Step 6: The platform can comment on the privacy and cybersecurity safeguards; following the platform's comments, the Office makes a final determination re: the safeguards. (Sec. 4).
Social Media Data Act	A covered platform must maintain, and **grant academic researchers and the Commission access** to, an **ad library** that contains in a **searchable, machine readable** format. (Sec. 2(a)(1))
Digital Services Oversight and Safety Act	The FTC establishes a "**research certification process**" under which an organization can apply and be qualified as a host organization and an individual associated with a host organization can apply and be certified as a certified researcher. (Sec. 10(b)) The FTC issues **regulations specifying the manner in which researchers will access information** from covered platforms. (Sec. 10(c)(1) & 10(c)(4)) The FTC must consider, among other things, **size and sampling techniques** used to create data sets, under what circumstances **APIs** are required, and designate "**secure facilities and computers** to analyze information through a Federally Funded Research and Development Center" established by the Act. (Sec. 10(c)(4).

CENTER FOR DEMOCRACY & TECHNOLOGY

Kids Online Safety Act	The NTIA must establish a program under which a researcher can apply for access to data and the NTIA can approve their application. (Sec. 7(b)(1)-(4)) For applications that are approved, a covered platform must provide to a qualified researcher access to data assets **through online databases, application programming interfaces, and data files** as appropriate for the qualified researcher to undertake public interest research. (Sec. 7(b)(3)(A)(ii))
DSA Art. 31	Researchers would be vetted and awarded the status of "vetted researchers" by the Digital Services Coordinator of establishment. (Art. 31, para. 4) Researchers can also apply to become a "vetted researcher" to the Digital Services Coordinator of the Member State of the research organisation to which they are affiliated. The DSC of the Member State would assess the application and send the assessment and application to the DSC of establishment, which makes the final decision on whether to award the status of "vetted researcher." (Art. 31, para. 4a) Access to data would be provided through "**appropriate interfaces**" specified in the researcher's request, including **online databases** or **application programming interfaces.** (Art. 31 para. 3) **More details TBD**: The Commission must adopt **delegated acts** laying down, among other things, "the technical conditions under which providers of very large online platforms are to share data . . . ." (Art. 31 para. 5)
EDMO Draft Code of Conduct	Step 1: DSOs make available **codebooks** to describe the data that is available. (Part II, Section 2) Step 2: Researchers submit a **research proposal** to the DSO from which they are requesting data. (Part II, Section 3). The research proposal must include a **Data Needs Management Plan (DNMP)** (Part II, Section 4) with an explanation of the **specific purpose of the data requested**, a **risk assessment** (Part II, Section 5), and **proposed safeguards** (Part II, Section 6), among other information. The DNMP must be **approved in writing by the researcher's institutional data protection officer**. The research proposal and DNMP must also undergo **ethical and methodological peer review**, and researchers must obtain a **certification** of the reviews and submit the certification to the DSO. (See Part II, Section 7)

	Step 3: **The DSO reviews** the research proposal to ensure "(i) the proposed processing is for qualifying research under this Code, and (ii) that appropriate safeguards for data subjects' rights and freedoms, and technical and organisational measures, are in place to enable them to rely on the research exemptions in the GDPR." (Part II, Section 8) Step 4: The DSO and researcher enter into a **data sharing agreement**. Note: The report accompanying the draft Code of Conduct **strongly recommends that an independent intermediary body be created to oversee and implement the processes envisioned by the Code.** The independent intermediary body could (a) certify that researchers are qualified and competent to perform the research, (b) verify that the research itself is qualified under the Code, and (c) provide these certifications to the platforms and any other appropriate parties. It could also review and certify, per Part II of the Code, that appropriate technical and organisational safeguards are put in place by both platforms and researchers. Finally, it could "serve an advisory function to help facilitate access to data for researchers as provided for in Article 31 in the Digital Services Act." (Report at p.12).
American Data Privacy and Protection Act	Research must adhere to the **regulations for human subject research in 45 C.F.R. § 46**, which requires **Institutional Review Board approval of research involving human subjects**. (Sec. 101(b)(9)(A)(iii), 45 C.F.R. 46, Subpart A).

CENTER FOR DEMOCRACY & TECHNOLOGY

VII. Is there a safe harbor for independent methods of data access?

Platform Accountability and Transparency Act	**Yes**. No civil or criminal liability for **any person** for **collecting covered information** as part of a **newsgathering or research project** on a platform. (Sec. 11). Conditions: Only applies to "**covered methods of digital investigation**"; purpose must be to **inform the general public about matters of public concern**, and the information in fact is used only that way; the person takes **reasonable measures to protect the privacy** of the platform's users; w/r/t research accounts, the person takes reasonable measures to **avoid misleading users**; and the project **does not materially burden the technical operation of the platform.** (Sec. 11). **"Covered method of digital investigation"** = **TBD** by FTC regulations, but must include collection of data through automated means, through data donation, or through research accounts. (Sec. 11). **"Covered information"** = **publicly available** information, information about **ads**, **other information TBD** by FTC that **does not unduly burden user privacy.** (Sec. 11).
Social Media Data Act	**No**.
Digital Services Oversight and Safety Act	**Yes. Certified researchers** granted immunity for liability under **state, federal, and local law** for **violating platform's TOS** for two specified research activities: creating a research account (if researcher takes reasonable means to avoid misleading users and does not burden technical operation of platform) and data donation with informed consent of users. (Sec. 10(c)(10)) Also **prohibits a covered platform from discriminating against a certified researcher** in the provision of services because of those two research activities. (Sec. 10(c)(10)).
Kids Online Safety Act	**Yes.** No cause of action for **violating platform's TOS** may be brought based on actions a researcher takes while collecting data assets as part of public interest research regarding harms to minors. (Sec. 7(c))
DSA Art. 31	**No**.

EDMO Draft Code of Conduct	**No.**
American Data Privacy and Protection Act	**No.**