DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 241204–0309]

RIN 0660–XC064

Ethical Guidelines for Research Using Pervasive Data

AGENCY: National Telecommunications and Information Administration (NTIA), Department of Commerce.

ACTION: Notice, request for public comments.

SUMMARY: The National Telecommunications and Information Administration (NTIA) is seeking public input on the potential writing of ethical guidelines for the use of ''pervasive data'' in research. ''Pervasive data'' refers to data about people gathered through online services. NTIA will rely on these comments, along with stakeholder engagements, in considering whether to draft and issue non-binding guidelines to assist researchers working with pervasive data. Such guidelines, if warranted, would detail how researchers can work with pervasive data while meeting ethical expectations of research and protecting individuals' privacy and other rights.

DATES: Interested persons are invited to submit comments on or before January 15, 2025.

ADDRESSES: All electronic public comments on this action, identified by *Regulations.gov* docket number NTIA–2024–0004, may be submitted through the Federal eRulemaking Portal at *www.regulations.gov.* The docket established for this request for comments can be found at *www.regulations.gov,* NTIA–2024–0004. Please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. All comments received are a part of the public record and will generally be posted to *Regulations.gov* without change. All personally identifiable information (*e.g.,* name, address) voluntarily submitted by the commenter may be publicly accessible. Information obtained as a result of this notice may be used by the federal government for program planning on a non-attribution basis.

FOR FURTHER INFORMATION CONTACT: Please direct questions regarding this Request for Comments to Emma Llansó, NTIA, 1401 Constitution Avenue NW, Washington, DC 20230, at *ellanso@ntia.gov* or 202–482–3821. Please direct media inquiries to NTIA's Office of Public Affairs, telephone: (202) 482–7002; email: *press@ntia.gov.*

SUPPLEMENTARY INFORMATION:

Overview

The National Telecommunications and Information Administration (NTIA) is seeking input from the public on the potential writing of ethical guidelines for the use of ''pervasive data'' in research. ''Pervasive data'' refers to data about people gathered through online services.[1] Researchers have leveraged pervasive data to better understand human behavior, societal forces, public health, and the impact of the technology that surrounds us. These insights are essential for informing policy in the digital age, and researchers and organizations have called for ethical guidelines to help ensure this work is done responsibly.[2] Such guidelines, if warranted, would detail how independent third-party researchers [3] can work with pervasive data while meeting ethical expectations of research and protecting individuals' privacy and other rights. The goal of ethical guidelines would be to outline principles and best practices that researchers, research institutions, data intermediaries,[4] and online service providers can choose to follow when involved in research with pervasive data. Any such ethical guidelines may be a reference for research conducted solely within the United States (U.S.) or through international collaborations.

NTIA will rely on these comments, along with engagements with researchers, civil society, research institutions, industry, and other government bodies, to consider whether to draft and issue guidelines to assist researchers working with pervasive data. The ethical guidelines outlined for consideration in this Request for Comments would be non-binding and would not supersede any existing laws or regulations, or pre-empt future laws. For example, human subjects research conducted or supported by one of the U.S. government departments or agencies that have adopted the Federal Policy for the Protection of Human Subjects ('Common Rule') [5] would need to adhere to any applicable regulatory requirements. Federal agencies and federal data are bound by additional laws and regulations, which these voluntary ethical guidelines would not supersede.[6]

Background

Research with pervasive data is essential in efforts to understand the impact of technology on society. For example, the Kids Online Health and Safety Task Force Report and the Surgeon General's Youth Mental Health Advisory both emphasize that access to pervasive data, paired with privacy safeguards and ethical research guidelines, is essential to understanding technology's impact on children.[7]

[1] The term *pervasive data* is intended to mean data about people—user-contributed, observed, derived, or inferred—collected through online services regardless of the extent to which the data is publicly available, is aggregated, or could lead to the identification of an individual. Pervasive data may include text, images, videos, biometric information, information about a data subject's behavior (purchases, financial standing, media consumption, search history, medical conditions, location, etc.), and other information that makes up a person's digital footprint. *Online services* may include a wide range of information technologies throughout the technology stack/technical infrastructure, including but not limited to web-based monitoring tools, content delivery networks, blockchain technology, digital labor platforms, education technology, Internet of Things devices, connected cars, wearable devices, mobile sensors, data brokers, streaming services, search engines, online marketplaces, social media platforms, and AI systems. The term pervasive data is informed by research conducted under NSF Grant Award Number 1144934 (*https://www.nsf.gov/awardsearch/showAward?AWD_ID=1144934*).

[2] *See e.g.* Michael Zimmer, *Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity,* Social Media + Society 4, no. 2 (2018), *https://doi.org/10.1177/2056305118768300;* aline shakti franzke et al., *internet Research: Ethical Guidelines 3.0, Association of internet Researchers* (2020), *https://aoir.org/reports/ethics3.pdf.*

[3] The ethics and privacy guidelines described for consideration in this Request for Comments focus on the flow of data from online service providers to independent researchers that operate outside of the online service provider and are often affiliated with an academic or non-profit institution.

[4] The term *data intermediary* is intended to describe an independent entity that is operated specifically to facilitate data access and sharing under commercial or non-commercial agreements between researchers and online service providers or that evaluates and approves researcher requests for access to designated subsets of stored pervasive data. *See* Organisation for Economic Co-operation and Development, *Data Stewardship, Access, Sharing, and Control: A Going Digital III module synthesis report,* DSTI/CDEP(2022)6/FINAL (2023) at 37.

[5] *See* Office for Human Research Protections (OHRP), *Federal Policy for the Protection of Human Subjects ('Common Rule'),* OHRP (June 23, 2009), *https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html.*

[6] *See, e.g.,* the Privacy Act of 1974, 5 U.S.C. 552a (1974); the Paperwork Reduction Act of 1980, 44 U.S.C. 3501–3521 (1980); the Federal Information Security Modernization Act of 2014, Public Law 113–283 (2014); the E-Government Act of 2002, 44 U.S.C. 101 (2002).

[7] Kids Online Health and Safety Task Force, *Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry,* Substance Abuse and Mental Health Services Administration (July 19, 2024), *https://www.samhsa.gov/kids-online-health-safety-task-force/kohs-report-safe-internet-use;* Office of the Assistant Secretary for Health (OASH). *Surgeon General Issues New Advisory About Effects Social Media Use Has on Youth Mental Health,* OASH (May 23, 2023), *https://www.hhs.gov/about/news/*

Pervasive data is also crucial to enabling responsible research in other fast-moving technologies. For example, the National Artificial Intelligence (AI) Initiative Act of 2020, along with the CHIPS and Science Act of 2022, include landmark investments in AI research to advance the use of trustworthy AI.[8] Such research often relies on pervasive data and should be conducted ethically.[9]

Research with pervasive data is widespread and in high demand. To better understand the impact of technology on society, researchers have developed methods for accessing pervasive data, including large-scale collection of publicly available information, entering into agreements with online service providers, and managing collections of user-contributed data.[10] Policymakers in the U.S. and globally have called for providers of online services to make data available to researchers.[11] European regulators recently enacted the Digital Services Act, which mandates that Very Large Online Platforms share pervasive data with researchers to study systemic risks in the information environment.[12] However, the risks to the rights and welfare of individuals associated with the use of pervasive data for research are nuanced and context-specific. This Request for Comments aims to explore these complexities and work toward more ethical practices for researchers working with pervasive data.

Discussion of research ethics has a long history, and the U.S. government has worked to shape well-recognized principles.[13] In 1979, the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research released the Belmont Report, which outlined three principles: respect for persons, beneficence, and justice.[14] These principles were the foundation of regulations implemented in 1981 by both the Department of Health and Human Services (HHS) and the Food and Drug Administration.[15] Today, a version of the Common Rule, which was revised in 2017, has been adopted by 21 Federal departments and agencies.[16] The regulations mandate that institutions engaged in nonexempt human subjects research supported or conducted by a Common Rule department or agency obtain institutional review board (IRB) approval before research can begin. With certain exemptions, IRBs review human subjects research according to specific criteria which are grounded in the Belmont Report's ethical principles, including a requirement for researchers to obtain informed consent from study participants unless the research is eligible for a waiver of informed consent.[17]

The Common Rule sometimes applies to research conducted on pervasive data. However, as with other broad categories of research, the Common Rule does not apply to the full range of research using pervasive data and was not designed to address all societal risks associated with research using pervasive data.[18] Specifically, the Common Rule applies to *human subjects research* which, in the context of online data, involves either obtaining information through an intervention or interaction with the living individual(s) about whom the research is conducted, or obtaining, using, studying, analyzing, or generating identifiable private information about the living individual(s).[19] Therefore, the secondary use of only non-identifiable data in research, for example, would generally not be subject to the Common Rule's requirements, even for research that is federally supported or conducted.[20] Further, some research conducted with identifiable private information may meet the criteria of one or more categories of exemption from the Common Rule requirements, which

2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html.

[8] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116–283, § Division E (2021). *https://www.congress.gov/bill/116th-congress/house-bill/6395/text;* CHIPS and Science, Public Law 117–167 (2022). *https://www.congress.gov/bill/117th-congress/house-bill/4346/text.*

[9] *See e.g.* National Institute of Science and Technology, *NIST Researchers Suggest Historical Precedent for Ethical AI Research,* NIST (February 15, 2024), *https://www.nist.gov/news-events/news/2024/02/nist-researchers-suggest-historical-precedent-ethical-ai-research.*

[10] *See e.g.* Jakob Ohme, et al., *Digital Trace Data Collection for Social Media Effects Research: APIs, Data Donation, and (Screen) Tracking,* Communication Methods and Measures 18, no. 2, 124–41 (April 2, 2024), *https://doi.org/10.1080/19312458.2023.2181319;* Michael W. Wagner, *Independence by Permission,* Science 381, no. 6656, 388–91 (July 28, 2023), *https://doi.org/10.1126/science.adi2430.*

[11] *See e.g.* The White House, *U.S–EU Joint Statement of the Trade and Technology Council,* The White House (April 5, 2024), *https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/05/u-s-eu-joint-statement-of-the-trade-and-technology-council-3/;* UNESCO, *Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multi-Stakeholder Approach,* UNESCO (2023), *https://unesdoc.unesco.org/ark:/48223/pf0000387339.*

[12] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L § Article 40 (2022), *http://data.europa.eu/eli/reg/2022/2065/oj/eng.*

[13] In addition to ethical guidelines, laws regulating privacy are also relevant for researchers to consider. While the U.S. does not currently have an over-arching data protection law, sectoral laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), Electronic Communications Privacy Act (ECPA), Federal Trade Commission Act, Digital Millennium Copyright Act (DMCA) and other provisions in Title 17 of the United States Code, Title 9 of the United States Code, Title 18 of the United States Code, the 21st Century Cures Act, and other statutes may be relevant for researchers in certain contexts. Additionally, some online service providers may be under federal consent orders that affect how they can collect and share their users' data, including with researchers.

[14] Office for Human Research Protections (OHRP), *The Belmont Report,* OHRP (January 28, 2010), *https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html.* For more history on human subjects research, see Michael G. White, *Why Human Subjects Research Protection Is Important,* The Ochsner Journal 20, no. 1, 16–33 (2020), *https://doi.org/10.31486/toj.20.5012.*

[15] Office for Human Research Protections (OHRP), *Federal Policy for the Protection of Human Subjects ('Common Rule'),* OHRP (June 23, 2009), *https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html.*

[16] Office for Human Research Protections (OHRP), *Federal Policy for the Protection of Human Subjects ('Common Rule'),* OHRP (June 23, 2009), *https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html.*

[17] Office for Human Research Protections (OHRP), *2018 Requirements (2018 Common Rule,* OHRP (March 7, 2017), *https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/revised-common-rule-regulatory-text/index.html.*

[18] *See* A. Michael Froomkin, Big Data: Destroyer of Informed Consent, 21 YALE J.L. & TECH. 27 (2019). *See also,* Edmund G Howe III, Falicia Elenberg, Ethical Challenges Posed by Big Data, 17 Innov Clin Neurosci. 24–30 (2020). *See also,* Jessica Vitak et al., *Beyond the Belmont Principles: Ethical Challenges, Practices, and Beliefs in the Online Data Research Community,* In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, 941–53. CSCW '16. New York, NY, USA: Association for Computing Machinery (2016), *https://doi.org/10.1145/2818048.2820078;* Michael S. Bernstein, et al., *ESR: Ethics and Society Review of Artificial Intelligence Research,* arXiv/Stanford University (July 9, 2021), *https://doi.org/10.48550/arXiv.2106.11521.*

[19] 45 CFR 46.102. Note that the Common Rule also includes definitions of both ''private information'' and ''identifiable private information.'' Specifically, ''[p]rivate information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (*e.g.,* a medical record)'' and ''[i]dentifiable private information is private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.'' Also, note that not all Common Rule signatories incorporate the Common Rule regulations into their own agency-specific regulations.

[20] Office for Human Research Protections (OHRP), *Human Subject Regulations Decision Charts: 2018 Requirements* (December 28, 2010), *https://www.hhs.gov/ohrp/regulations-and-policy/decision-charts-2018/index.html.*

would mean that IRB approval is not required.[21]

Recognizing the need for ethical guidelines beyond the Belmont Report and Common Rule, multiple institutions have tried to fill the gap. Starting in 2009, the Department of Homeland Security, which is a signatory to the Common Rule, engaged lawyers and computer scientists to draft a set of non-binding ethical guidelines for computer security and network measurement research. This led to the Menlo Report in 2012, which applied the Belmont Principles to network and security research and added an additional principle: respect for law and public interest.[22] The Association of internet Researchers (AoIR) has gone through several versions of ethical guidelines targeted at researchers and organizations involved in studying people in internet-related venues.[23] The American Statistical Association (ASA) has developed guidelines focused on ''statistical practice'', which includes, among other things, designing data collection, processing data, and analyzing data.[24] The ASA guidelines also include the development and deployment of algorithms and AI models.

As technology has continued to advance, online services have developed the capacity to collect data on human behavior at massive scales.[25] Building on the government's commitment to ethical research, NTIA is considering drafting ethical guidelines for research involving pervasive data, which requires considerations beyond those enshrined in existing ethics regulations and practices.[26]

Pervasive data can be drawn from global networks and may be analyzed by an international community of researchers. Therefore, it is increasingly important to use a global lens to address ethical issues in pervasive data. Advancements in research using pervasive data may benefit from international collaboration and agreed-upon norms for ethical research and the protection of privacy and other rights. For example, the U.S.-EU [27] Trade and Technology Council Working Group on Tech Platform Governance recently announced a shared commitment to advance data access for researchers and has begun discussing such principles.[28]

Risks created by research vary throughout the lifecycle of a project, from research design to dissemination.[29] Users of commercial online services often do not understand or have control over how their data will be used.[30] Previous research has further found that *researchers'* use of pervasive data for research is often not consistent with users' expectations, even if the information involves public social media posts.[31] Risks to data subjects presented by research with pervasive data include reidentification of anonymous user accounts; release or inference of information that can be used to perpetuate a range of privacy and other individual-level harms, including fraud, impersonation, discrimination, reputational harms, and emotional distress; and decreased willingness to post and access information online and engage in the digital economy.[32] Research using pervasive data also has the potential to generate societal and/or systemic risks beyond the individual-level risks to data subjects. These risks include the potential to undermine trust in the research ecosystem when users learn about unethical research,[33] further disadvantage historically disadvantaged groups,[34] cause negative impacts on the environment,[35] and create risks from the products of that research, such as machine learning models being used out of context.[36] While researchers across

[21] Office for Human Research Protections (OHRP), *Human Subject Regulations Decision Charts: 2018 Requirements* (December 28, 2010), *https://www.hhs.gov/ohrp/regulations-and-policy/decision-charts-2018/index.html.*

[22] *See* Homeland Security, *Menlo Report: Ethical Principles Guiding Information and Communication Technology Research* (August 3, 2012). *See also,* Megan Finn and Katie Shilton, *Ethics Governance Development: The Case of the Menlo Report,* Social Studies of Science 53, no. 3, 315–40 (2023), *https://doi.org/10.1177/03063127231151708.*

[23] *See* aline shakti franzke et al., *internet Research: Ethical Guidelines 3.0, Association of internet Researchers* (2020), *https://aoir.org/reports/ethics3.pdf.*

[24] *See Ethical Guidelines for Statistical Practice,* American Statistical Association (February 2022), *https://www.amstat.org/docs/default-source/amstat-documents/ethicalguidelines.pdf.*

[25] *See, e.g.,* Patrick S. Park, et al., *The Strength of Long-Range Ties in Population-Scale Social Networks,* Science 362, no. 6421 (December 21, 2018), *https://doi.org/10.1126/science.aau9735. See also,* Claire E. Robertson, et al., *Negativity Drives Online News Consumption,* Nature Human Behaviour 7, no. 5, 812–22 (May 2023), *https://doi.org/10.1038/s41562-023-01538-4. See also,* Markus Schläpfer, et al., *The Universal Visitation Law of Human Mobility,* Nature 593, no. 7860, 522–27, (May 2021), *https://doi.org/10.1038/s41586-021-03480-9.*

[26] *See e.g.* The World Medical Association, *WMA Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks* (October, 2016), *https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/.* For example, The World Medical Association also codified the Declaration of Taipei in 2016, which includes ethical principles for research with health databases.

[27] European Union.

[28] *See e.g.* The White House, *U.S.-EU Joint Statement of the Trade and Technology Council,* The White House (May 31, 2023), *https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/;* U.S.- EU Trade and Technology Council (TTC), *Joint Principles on Combatting Gender Based Violence in the Digital Environment √ Shaping Europe's Digital Future* (April 5, 2024), *https://digital-strategy.ec.europa.eu/en/library/us-eu-trade-and-technology-council-ttc-joint-principles-combatting-gender-based-violence-digital.*

[29] *See* aline shakti franzke et al., *internet Research: Ethical Guidelines 3.0, Association of internet Researchers* (2020), *https://aoir.org/reports/ethics3.pdf.*

[30] *See e.g.* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics,* 11 NW. J. TECH. & INTELL. PROP. 239 April 2013; Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services,* Information, Communication & Society 23, no. 1, 128–4 (January 2, 2020), *https://doi.org/10.1080/1369118X.2018.1486870;* Transparency and various forms of user control are at the heart of the Fair Information Practice Principles, which were first articulated in a 1973 Federal Government report from the Department of Health, Education, and Welfare Advisory Committee, ''Records, Computers and the Rights of Citizens.'' *See FPC.gov, Fair Information Practice Principles (FIPPs)* (1973), *https://www.fpc.gov/resources/fipps/.*

[31] *See e.g.* Casey Fiesler & Nicholas Proferes, *Participant' Perceptions of Twitter Research Ethics,* Social Media + Society 4, no. 1 (2018), *https://doi.org/10.1177/2056305118763366;* Michael Zimmer, *But the Data Is Already Public': On the Ethics of Research in Facebook,* Ethics and Information Technology 12, no. 4, 313–25 (December 1, 2010), *https://doi.org/10.1007/s10676-010-9227-5.*

[32] *See* Michael Zimmer, *Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity,* Social Media + Society 4, no. 2 (2018), *https://doi.org/10.1177/2056305118768300;* Daniel J. Solove & Danielle Keats, *Privacy Harms,* GW Law Faculty Publications & Other Works. 1534 (2021), *https://scholarship.law.gwu.edu/faculty_publications/1534.*

[33] *See* Mary L. Gray, *A Human Rights Framework for AI Research Worthy of Public Trust,* Issues in Science and Technology, May 21, 2024, *http://issues.org/ai-ethics-research-framework-human-rights-gray/;* Danah Boyd, *Untangling Research and Practice: What Facebook's 'Emotional Contagion' Study Teaches Us.* Research Ethics 12, no. 1, 4–13 (2016), *https://doi.org/10.1177/1747016115583379.*

[34] *See* Jonathan Herington, et al., *Ethical Imperatives for Working With Diverse Populations in Digital Research,* Journal of Medical internet Research 25, no. 1 (September 18, 2023), *https://doi.org/10.2196/47884;* Alex Thompson, et al., *Ethical Considerations and Challenges for Using Digital Ethnography to Research Vulnerable Populations,* Journal of Business Research 124, 676–83 (January 1, 2021), *https://doi.org/10.1016/j.jbusres.2020.02.025.*

[35] *See* Jude Coleman, *AI's Climate Impact Goes beyond Its Emissions, Scientific American* (Dec 7, 2023), *https://www.scientificamerican.com/article/ais-climate-impact-goes-beyond-its-emissions/; See also Irene* V. *Pasquetto, What Is Research Data 'Misuse'? And How Can It Be Prevented or Mitigated?,* Journal of the Association for Information Science and Technology (July 27, 2024), *https://doi.org/10.1002/asi.24944.*

[36] *See* Kristen K. Greene et al., *Avoiding Past Mistakes in Unethical Human Subjects Research: Moving From Artificial Intelligence Principles to Practice,* Computer 57, no. 2, 53–63 (February 2024), *https://doi.org/10.1109/MC.2023.3327653;* Anja Bechmann & Bendert Zevenbergen, *AI, and*

the country have taken voluntary measures to consider risks to data subjects in their research with pervasive data, the U.S. does not have a recognized set of shared guidelines.[37]

This Request for Comments considers ethical issues and risks to privacy and other rights, and mitigation strategies throughout the lifecycle of a research project, from research design, data acquisition, and access, data processing, and analysis to dissemination.[38] The questions recognize that the research design phase allows researchers to reflect on the potential for harm to data subjects, society, and themselves; these considerations should be revisited throughout the remaining phases of research.[39]

Definitions

For purposes of responding to this Request for Comments, please refer to the following definitions:

The term pervasive data is intended to mean data about people—user-contributed, observed, derived, or inferred—collected through online services regardless of the extent to which the data is publicly available, is aggregated, or could lead to the identification of an individual. Pervasive data may include text, images, videos, biometric information, information about a data subject's behavior (purchases, financial standing, media consumption, search history, medical conditions, location, etc.), and other information that makes up a person's digital footprint.[40]

Online services may include a wide range of information technologies throughout the technology stack/technical infrastructure, including but not limited to web-based monitoring tools, content delivery networks, blockchain technology, digital labor platforms, education technology, Internet of Things devices, connected cars, wearable devices, mobile sensors, data brokers, streaming services, search engines, online marketplaces, social media platforms, and AI systems.[41]

The term *data intermediary* is intended to describe an independent entity that is operated specifically to facilitate pervasive data access and sharing under commercial or non-commercial agreements between researchers and online service providers or that evaluates and approves researcher requests for access to designated subsets of stored pervasive data.

A *data subject,* for the purposes of this Request for Comments, is an individual whose personal information is contained in the pervasive data. The individual may be a digital device user who creates the information or who sets up and manages an account, or they could be an individual whose data is captured in the user's information (*e.g.,* a child in a parent's photo, a visitor to a home that has smart devices, an electronically-monitored employee, or a passenger in a vehicle with tracking technology). Data subjects may or may not be ''human subjects'' as defined in the Common Rule.

Instructions for Commenters

Through this Request for Comments, we hope to gather information on the following questions and the broader topic outlined above. These questions are not exhaustive and commenters are invited to provide input on relevant questions not asked below. Commenters are not required to respond to all questions. When responding to one or more of the questions below, commenters are requested to include a question number with each part of their response. Commenters should include a page number on each page of their submissions. Commenters are welcome to provide specific actionable proposals, frameworks, rationales, and relevant facts.

Questions

1. What are the potential benefits of developing national-level ethical guidelines for researchers collecting, analyzing, and sharing pervasive data?

2. What are the potential drawbacks of developing national-level ethical guidelines for researchers collecting, analyzing, and sharing pervasive data?

3. To what extent does the definition of *pervasive data* in this Request for Comments capture the appropriate scope for national ethical guidelines?

a. Are there particular types of data or other digital artifacts [42] that should be carefully considered or included/excluded in the definition?

b. Are there pre-existing similar definitions, similar to the one provided, that should be considered?

4. What are some existing barriers to accessing pervasive data?

a. What are examples of research questions, if any, that are challenging to answer because of the barriers to accessing pervasive data? [43] If possible, also explain why other methodological approaches and data types are insufficient for answering those questions.

b. If those barriers were removed, what would be the potential benefits and additional risks to society and individuals, if any?

5. What data held by online services would be most valuable to the public interest if researchers were able to access it?

6. Consent and autonomy are key principles in human subjects research ethics. However, users of online services may be required to divulge certain personal information and/or have no ability to freely make decisions about its use.[44] How should researchers working with pervasive data consider consent and autonomy?

a. What, if any, would be an appropriate consent model for research

Machine Learning: internet Research Ethics Guidelines, IRE 3.0 Companion 6.1, Association of Internet Researchers, 33–49 (2020), *https://aoir.org/reports/ethics3.pdf.*

[37] *See* Jessica Vitak et al., *Beyond the Belmont Principles: Ethical Challenges, Practices, and Beliefs in the Online Data Research Community,* In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, 941–53. CSCW '16. New York, NY, USA: Association for Computing Machinery (2016), *https://doi.org/10.1145/2818048.2820078;* Katie Shilton & Sheridan Sayles, *We Aren't All Going to Be on the Same Page about Ethics': Ethical Practices and Challenges in Research on Digital and Social Media,* In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), 1909–18. HICSS '16. USA: IEEE Computer Society (2016), *https://doi.org/10.1109/HICSS.2016.242.* See also Madhulika Srikmar et al., *Advancing Ethics Review Practices in AI Research.* Nature Machine Intelligence 4, no. 12, 1061–64 (December 2022), *https://doi.org/10.1038/s42256-022-00585-2.*

[38] *See* aline shakti franzke et al., *internet Research: Ethical Guidelines 3.0, Association of internet Researchers* (2020), *https://aoir.org/reports/ethics3.pdf.*

[39] *See e.g.* Katie Shilton, et al., *Excavating Awareness and Power in Data Science: A Manifesto for Trustworthy Pervasive Data Research,* Big Data & Society 8, no. 2 (2021), *https://doi.org/10.1177/20539517211040759;* Annette Markham, *Ethic as Method, Method as Ethic: A Case for Reflexivity in Qualitative ICT Research,* Journal of Information Ethics 15, no. 2, 37–54 (November 1, 2006), *https://doi.org/10.3172/JIE.15.2.37.*

[40] This project does not include biospecimens as pervasive data.

[41] For the purpose of this project, online services do not include health plans, healthcare clearinghouses, or healthcare providers as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

[42] Here, the term *digital artifact* is intended to include digital information that may not immediately be recognized as *data,* regardless of whether the information satisfies any particular definition of *data.* Examples might include AI models or systems, algorithm-to-human response patterns, or digital items exchanged in a marketplace.

[43] *See e.g.* U.S -EU Trade and Technology Council, *Commission and White House Published Workshop Report on Researcher Access to Online Platform Data and Its Role for Research on Gender-Based Violence Online | Shaping Europe's Digital Future, European Commission* (May 6, 2024), *https://digital-strategy.ec.europa.eu/en/news/commission-and-white-house-published-workshop-report-researcher-access-online-platform-data-and-its.*

[44] *See, e.g.,* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics,* 11 Nw. J. Tech. & Intell. Prop. 239 (2013), *https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/.*

with pervasive data? How and how often should consent occur?

b. Are there alternative models to traditional consent that either support autonomy or provide protections for data subjects in cases where autonomy is limited?

c. How, if at all, is user autonomy influenced by context, such as the need to use online services for school, work,[45] or socializing?

7. What ethical issues and risks to privacy and other rights, and mitigation strategies, should be considered during the research design phase?

a. Users' concerns about researcher data access vary based on contextual factors.[46] What contextual factors increase or alter the risks to data subjects in research using pervasive data?[47]

b. What factors contribute to a user's expectations of privacy on an online service?[48]

c. What power differences exist between researchers and data subjects, or between online service providers and data subjects, that could create unique risks and potential for harm.[49] How should these differences be considered and mitigated during the research design phase?

d. What unique risks affect children and youth? How do these differ depending on their gender, age, developmental capabilities, and other factors?[50] How does this impact the way researchers should think about risks when using pervasive data that includes young data subjects, especially those who are not legally adults? What are best practices when working with pervasive data created by or containing information about children and youth? What is the appropriate role of parents/guardians in such research?

e. What other vulnerable communities or vulnerability risk factors warrant additional consideration when conducting research with pervasive data? Please explain.

f. How might researchers account for changes in data subject status over time (*e.g.,* aging into an adult category; dying; transitioning gender; changing citizenship, employment, disability, or veteran status)? How should researchers consider privacy and other rights when data subjects change status?

g. When considering ethical issues and risks to privacy and other rights for data subjects, how should researchers consider differences in views across individuals, communities, ethnicities, nationalities, languages, cultures, socioeconomic status, employment status, and educational levels?

h. How can researchers best conduct research with pervasive data in a way that engages the community, users, and data subjects.[51] What are the best practices for such participatory research that uses pervasive data? What are the challenges and/or barriers to conducting participatory research? What important research questions cannot be answered using participatory mechanisms, and why?

i. What research conducted with pervasive data could pose societal-level risks beyond those to the researcher and data subject individually?[52] How should researchers assess and mitigate societal-level risks in comparison with potential benefits during the design phase?

j. How should ethical guidelines address risks to researchers?[53] What risks to researchers are currently difficult for researchers to mitigate on their own?

k. How, if at all, should ethical guidelines address methodological rigor, including the strength of the underlying research design and the confidence with which conclusions can be drawn?

l. How do changes in the norms, features, policies, and use of online services impact the ability to have well-understood and accepted methods for the collection, study design, and analysis of pervasive data? How can researchers adapt to changes in online services? How can online service providers support researchers in ethical research with pervasive data?

8. What are the risks and mitigation measures related to pervasive data acquisition and access?

---

[45] *See, e.g.,* Ifeoma Ajunwa, Kate Crawford & Jason Schultz, Limitless Worker Surveillance, 105 Calif. L. Rev. 735 (2017), *https://heinonline.org/HOL/LandingPage?handle=hein.journals/calr105&div=28&id=&page=.*

[46] *See* Michael Zimmer, *Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity,* Social Media + Society 4, no. 2 (2018), *https://doi.org/10.1177/2056305118768300;* Sarah Gilbert, *When Research Is the Context: Cross-Platform User Expectations for Social Media Data Reuse,* Big Data & Society 10, no. 1 (2023), *https://doi.org/10.1177/20539517231164108;* Kristen E. Martin, *Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract,* Journal of Business Ethics 111, no. 4, 519–39 (December 1, 2012), *https://doi.org/10.1007/s10551-012-1215-8;* Kirsten Martin & Katie Shilton, *Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices,* The Information Society, 32:3, 200–216 (2016), *https://doi.org/10.1080/01972243.2016.1153012.*

[47] Considerations may include, for example, the type of online service (social media, marketplace, infrastructure), the type of data collected (comments, photos, geolocation), demographics of the data subjects as a group, the situation in which data is collected (*e.g.,* in the workplace), online service features, values and norms on the online service, feasibility of reidentification or research topic, how research output might be used for other purposes, and the data quality and fitness for purpose, *See, e.g.,* Russell T. Vought, Office of Management and Budget, *Memorandum re: Improving Implementation of the Information Quality Act* (April 24th, 2019), *https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-15.pdf.*

[48] Considerations may include, for example, high-profile accounts, audience settings, requirements that users log in to view content, encryption services, data sharing/linking provisions, and privacy policies. *See also* James M. Hudson & Amy Bruckman, ''*Go Away*'': *Participant Objections to Being Studied and the Ethics of Chatroom Research.* The Information Society 20, 2, 127–139 (April 2004), *https://doi.org/10.1080/01972240490423030.*

[49] *See* Matt Scherer, *Warning: Bossware May Be Hazardous to Your Health,* Center for Democracy & Technology (2021), *https://cdt.org/wp-content/uploads/2021/07/2021-07-29-Warning-Bossware-May-Be-Hazardous-To-Your-Health-Final.pdf;* Alexander Hertel-Fernandez, *Estimating the prevalence of automated management and surveillance technologies at work and their impact on workers' well-being,* Washington Center for Equitable Growth (n.d.), *https://equitablegrowth.org/research-paper/estimating-the-prevalence-of-automated-management-and-surveillance-technologies-at-work-and-their-impact-on-workers-well-being/;* Katie Shilton, et al., *Excavating Awareness and Power in Data Science: A Manifesto for Trustworthy Pervasive Data Research,* Big Data & Society 8, no. 2 (2021), *https://doi.org/10.1177/20539517211040759;* Anne Beaulieu & Adolfo Estalella, *Rethinking Research Ethics for Mediated Settings,* Information, Communication & Society 15, no. 1, 23–42 (2012), *https://doi.org/10.1080/1369118X.2010.535838.*

[50] *See, e.g.,* Office of the Assistant Secretary for Health (OASH). *Surgeon General Issues New Advisory About Effects Social Media Use Has on Youth Mental Health,* OASH (May 23, 2023), *https://www.hhs.gov/about/news/2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html.*

[51] *See e.g.* Nathan J. Matias & Merry Mou, *CivilServant: Community-Led Experiments in Platform Governance,* In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–13. CHI '18. New York, NY, USA: Association for Computing Machinery (2018), *https://doi.org/10.1145/3173574.3173583;* Tom Denison & Larry Stillman, Academic and Ethical Challenges in Participatory Models of Community Research, *Information, Communication & Society* 15, no. 7, 1037–54 (2012), *https://doi.org/10.1080/1369118X.2012.656138.*

[52] Societal-level risks may include risks to groups including historically marginalized or otherwise vulnerable communities, crowd workers (workers that label data and/or complete surveys), the environment, trust in research, national security, and others. *See* Anja Bechmann & Bendert Zevenbergen, *AI and Machine Learning: internet Research Ethics Guidelines, IRE 3.0 Companion 6.1,* Association of internet Researchers, 33–49 (2020), *https://aoir.org/reports/ethics3.pdf,* at 46; Michael S. Bernstein, et al., *ESR: Ethics and Society Review of Artificial Intelligence Research,* arXiv/Stanford University (July 9, 2021), *https://doi.org/10.48550/arXiv.2106.11521.*

[53] Risks to researchers may include but are not limited to, legal risks, challenges associated with studying content that evokes strong emotional reactions, or personal and professional hazards from performing public research on controversial topics. *See* aline shakti franzke et al., *internet Research: Ethical Guidelines 3.0, Association of internet Researchers* (2020), *https://aoir.org/reports/ethics3.pdf,* at 11; Aya Yadlin, *Understanding Researcher Risk and Safety in Qualitative Research Online,* Digital Society 3, no. 1, 4 (February 1, 2024), *https://doi.org/10.1007/s44206-024-00089-z.*

a. What are the risks to data subjects resulting from the methods used by researchers to access pervasive data? How do these risks vary based on the methods of access? [54]

b. Pervasive data often includes data subjects from different places, which may involve geographical region, legal jurisdiction, or culture. What limitations are posed by research with pervasive data that only includes data subjects from one place? How can quality research and data integrity be maintained in those cases? What best practices are available to ensure that the treatment of pervasive data across places remains consistent with the privacy expectations where the data were created?

c. What are the current best practices for de-identifying, pseudonymizing, or aggregating pervasive data? What practices exist to prevent or reduce the chance of re-identification of de-identified data? Where do these techniques fall short? What research questions may require identifiable data, and why? [55]

d. One common method for mitigating ethical issues and risks to privacy and other rights from sharing data is to provide controlled access.[56]

i. What are the challenges and opportunities associated with provisioning pervasive data through controlled access?

ii. What criteria should be used to evaluate a request for controlled access to pervasive data? [57]

iii. How can evaluation and approval procedures ensure access to pervasive data is non-discriminatory?

e. Under what conditions should data subjects be notified that their data is used for research? What are necessary and/or best practices for communicating with data subjects when their data is used for research? What barriers exist to notifying data subjects? [58]

i. When should informed consent be obtained from users or data subjects? What should be the differences between informed consent obtained for a specific project versus for commercial or general secondary use (*e.g.,* ''broad consent'')? What are the barriers to obtaining informed consent from users and data subjects?

ii. What practices exist to support autonomy of data subjects in ways that may differ from standard concepts of informed consent?

iii. What are the best ways to communicate with users and data subjects when their data is used for research?

9. What are the risks and mitigation measures that arise when processing and analyzing pervasive data? [59]

a. Researchers will sometimes combine pervasive data with other pervasive data or with non-pervasive data from other sources. How might this impact risks? What best practices exist to mitigate these risks?

10. What are the risks to privacy and other rights related to the dissemination and archiving of research outputs? What mitigation measures exist?

a. What steps should researchers take to protect data subjects or against societal-level harms prior to the dissemination of research outputs (publications, presentation slides, data visualization, datasets, AI/ML models, etc.)? [60]

b. Under what circumstances is it appropriate for an online service provider or data intermediary to have access to or review third-party research papers before they are submitted for publication? Are there circumstances where pre-publication review is inappropriate? [61]

c. Reproducibility can help promote trust in research.[62] What factors do/should researchers consider when deciding when/how to delete, store, share, or archive pervasive data? [63]

---

[54] See, *e.g.,* Sandvig, C., Hamilton, K., Karahalios, K., & Langbort, C. (2014). Auditing algorithms: Research methods for detecting discrimination on internet platforms. *Data and discrimination: converting critical concerns into productive inquiry,* 22(2014), 4349–4357. Responses may address the following methods as well as any others not listed: Web scrapers/crawlers, Application Programming Interfaces (APIs), clean rooms/data enclaves/secure computer interfaces, data donations through data portability features built within an online service, data donations through data exports provided to the user by request to the online service (a mandate in some data protection laws), data donations through a passive sensing app or browser extensions, contract-based partnerships between researchers and online service providers, contracts or data purchases between researchers and data intermediaries, virtual data centers, research data centers such as FSRDCs and FFRDCs, or workplace observation.

[55] *See* Jacob Metcalf & Kate Crawford. ''Where Are Human Subjects in Big Data Research? The Emerging Ethics Divide.'' *Big Data & Society* 3, no. 1 (2016), *https://doi.org/10.1177/2053951716650211. See also* Networking and Information Technology Research and Development Subcommittee of the National Science and Technology Council, *National Strategy to Advance Preserving Data and Analytics,* White House (March 2023), *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf.*

[56] *See* Christopher Morten et al., *Researcher Access to Social Media Data: Lessons from Clinical Trial Data Sharing,* 38 Berkeley Tech. L.J. 109 (2024), U of Michigan Public Law Research Paper No. 24–017 (April 1, 2024), *https://doi.org/10.2139/ssrn.4716353. See also,* Jeffrey Mervis, *Accessing U.S. Data for Research Just Got Easier,* Science (December 8, 2022), *https://doi.org/10.1126/science.adg2113;* National Institutes of Health, *Designating Scientific Data for Controlled Access | Data Sharing,* (Accessed August 31, 2024). *https://sharing.nih.gov/data-management-and-sharing-policy/protecting-participant-privacy-when-sharing-scientific-data/designating-scientific-data-for-controlled-access;* The National Secure Data Service Demonstration, *https://ncses.nsf.gov/initiatives/national-secure-data-service-demo;* The Standard Application Process, *https://ncses.nsf.gov/initiatives/standard-application-process.*

[57] Considerations might include, for example, the researcher (*e.g.,* affiliation), the research project (*e.g.,* research design, data security), the type of data (*e.g.,* identifiability, publicness, source, level of sensitivity, or information modality) or other factors.

[58] *See* National Institutes of Health, *Informed Consent for Research Using Digital Health Technologies,* 2024, *https://osp.od.nih.gov/wp-content/uploads/2024/05/DigitalHealthResource_Final.pdf;* Nathan J. Matais & Merry Mou, *CivilServant: Community-Led Experiments in Platform Governance,* In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–13. CHI '18. New York, NY, USA: Association for Computing Machinery (2018), *https://doi.org/10.1145/3173574.3173583;* Casey Fiesler & Nicholas Proferes, *Participant' Perceptions of Twitter Research Ethics,* Social Media + Society 4, no. 1 (2018), *https://doi.org/10.1177/2056305118763366.*

[59] Considerations may include assumptions made about the data, methodological flaws, misapplication of AI/ML systems, or statistical techniques used to analyze data. *See e.g.,* Anja Bechmann & Bendert Zevenbergen, *AI and Machine Learning: internet Research Ethics Guidelines, IRE 3.0 Companion 6.1,* Association of internet Researchers, 33–49 (2020), *https://aoir.org/reports/ethics3.pdf; See also* Zeynep Tufekci. *Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls,* Proceedings of the International AAAI Conference on Web and Social Media 8, no. 1, 505–14 (May 16, 2014), *https://doi.org/10.1609/icwsm.v8i1.14517.*

[60] *See e.g.* Anja Bechmann & Bendert Zevenbergen, *AI and Machine Learning: internet Research Ethics Guidelines, IRE 3.0 Companion 6.1,* Association of internet Researchers, 33–49 (2020), *https://aoir.org/reports/ethics3.pdf* at 43; Irene V. Pasquetto, *What Is Research Data 'Misuse'? And How Can It Be Prevented or Mitigated?,* Journal of the Association for Information Science and Technology (July 27, 2024), *https://doi.org/10.1002/asi.24944.*

[61] *See e.g.* U.S.-EU Trade and Technology Council, *Status Report: Mechanisms for Researcher Access to Online Platform Data | Shaping Europe's Digital Future,* Section 1.5.2 (April 5, 2024) *https://digital-strategy.ec.europa.eu/en/library/status-report-mechanisms-researcher-access-online-platform-data.*

[62] See *Moving towards Reproducible Machine Learning,* Nature Computational Science 1, no. 10, 629–30 (October 2021), *https://doi.org/10.1038/s43588-021-00152-6. See also* Committee on Reproducibility and Replicability in Science, et al., *Reproducibility and Replicability in Science,* Washington, DC, National Academies Press (2019), *https://doi.org/10.17226/25303.*

[63] Such factors might include but are not limited to: Treatment of user-created data that either the user or the online service provider deleted after the research project; Storage of data that includes information about data subjects that are not users; Length of time to store data following the conclusion of a research project and when and how to delete that data; Level of access to stored data (*e.g.,* is it available to the public or only researchers that have been granted access); Prior communication with data subjects, including whether data subjects received notice or gave informed consent; The types of data collected and the level of aggregation/deidentification performed; Restrictions or controls on how data can be

Continued

11. What existing ethical frameworks, such as those from professional organizations [64] or government agencies,[65] should be considered when drafting national-level ethical guidelines for research with pervasive data?

a. To what extent do existing frameworks apply to the collection and use of pervasive data?

b. What modifications of existing frameworks might be necessary to ensure that those frameworks are applicable to the needs of research with pervasive data?

12. What are the existing requirements and legal obligations that impact research with pervasive data?

a. What are the risks around research that uses pervasive data, if any, that currently fall beyond the usual considerations of IRBs operating under the Common Rule or FDA regulations?

b. What steps can be taken to ensure that potential new guidelines for research with pervasive data complement the existing regulatory framework for human subjects research?

c. How can research ethics guidelines be either integrated into existing workflows (such as IRB review processes) or given new workflows to ensure research is performed ethically and in a manner that protects individual privacy and other rights? [66]

d. To what extent do state laws, federal laws, or other legal obligations [67] create uncertainties, barriers, or appropriate protections for:

i. Online service providers to voluntarily share pervasive data with researchers?

ii. Data intermediaries' ability to store and provide access to pervasive data?

iii. Researchers' ability to collect and analyze pervasive data?

e. How are researchers constrained by provisions in online service's terms of service, such as online services' general end-user agreements or the terms associated with APIs and other researcher access programs? [68]

f. Pervasive data can include data subjects that reside outside of the U.S. and are therefore subject to different laws.[69] In what ways do international and foreign laws create uncertainties or barriers for:

i. Online service providers to voluntarily share pervasive data with researchers?

ii. Data intermediaries' ability to store and provision access to pervasive data?

iii. Researchers' ability to collect and analyze pervasive data?

13. What structured processes (questionnaires, rubrics, assessment frameworks) could be used to determine which techniques should be used to mitigate risks to data subjects and society in research that relies on pervasive data? [70]

14. How should ethical guidelines take into account future technological advances around research with pervasive data?

Dated: December 5, 2024.

Stephanie Weiner,

Chief Counsel, National Telecommunications and Information Administration.

[FR Doc. 2024–29064 Filed 12–10–24; 8:45 am]

BILLING CODE 3510–60–P

reshared or used, including whether data can be used for commercial purposes.

[64] *See, e.g., Ethical Guidelines for Statistical Practice,* American Statistical Association (February 2022), *https://www.amstat.org/docs/default-source/amstat-documents/ethicalguidelines.pdf. See also* aline shakti franzke, et al. Internet Research: Ethical Guidelines 3.0 (2020), *https://aoir.org/reports/ethics3.pdf.*

[65] *See, e.g., Artificial Intelligence And Worker Well-being: Principles And Best Practices For Developers And Employers,* Department of Labor (n.d.), *https://www.dol.gov/general/AI-Principles; Ethics Principles for Access to and Use of Veteran Data,* Department of Veterans Affairs (n.d.), *https://digital.va.gov/ethics-principles-for-access-to-and-use-of-veteran-data/;* NIST Privacy Framework (2020), *https://doi.org/10.6028/NIST.CSWP.01162020.*

[66] *See e.g.* Jessica Pater, et al., *No Humans Here: Ethical Speculation on Public Data, Unintended Consequences, and the Limits of Institutional Review,* Proc. ACM Hum.-Comput. Interact. 6, no. GROUP 38, 1–13 (January 14, 2022), *https://doi.org/10.1145/3492857.*

[67] In addition to the laws referenced in the Background, laws such as the Confidential Information Protection and Statistical Efficiency Act and Title 13 of the U.S. Code also set requirements for interactions with data.

[68] *See* U.S.-EU Trade and Technology Council, *Status Report: Mechanisms for Researcher Access to Online Platform Data | Shaping Europe's Digital Future,* Section 1.5.2 (April 5, 2024) *https://digital-strategy.ec.europa.eu/en/library/status-report-mechanisms-researcher-access-online-platform-data* at Section 1.5. *See also* Casey Fiesler, et al., *No Robots, Spiders, or Scrapers: Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service,* Proceedings of the International AAAI Conference on Web and Social Media 14, 187–96 (May 26, 2020), *https://doi.org/10.1609/icwsm.v14i1.7290. See also* Emil Chiauzzi, & Paul Wicks, *Digital Trespass: Ethical and Terms-of-Use Violations by Researchers Accessing Data From an Online Patient Community,* Journal of Medical internet Research 21, no. 2 (February 21, 2019), *https://doi.org/10.2196/11985.*

[69] *See* Office for Human Research Protections (OHRP), *Attachment B—European Union's General Data Protection Regulations* (March 13, 2018), *https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-b-implementation-of-the-european-unions-general-data-protection-regulation-and-its-impact-on-human-subjects-research/index.html.*

[70] See, for example, the following examples of frameworks, questionaries, rubrics, and assessment tools to help researchers reason through ethical principles and select best practices: Michael S. Bernstein, et al., *ESR: Ethics and Society Review of Artificial Intelligence Research,* arXiv/Stanford University (July 9, 2021), *https://doi.org/10.48550/arXiv.2106.11521;* Katie Shilton et al., *PERVADE Decision Support Tool—PERVADE,* University of Maryland (April 10, 2024), *https://pervade.umd.edu/2024/04/pervade-decision-support-tool/;* European Digital Media Observatory, *EDMO Releases Report on Researcher Access to Platform Data,* 76 (May 31, 2022), *https://edmo.eu/2022/05/31/edmo-releases-report-on-researcher-access-to-platform-data/;* Annette N Markham et al., *Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction,* Social Media + Society 4, no. 3 (2018), *https://doi.org/10.1177/2056305118784502;* Lorrie Cranor et al., *Conference Submission and Review Policies to Foster Responsible Computing Research,* Washington, DC Computing Research Association (2024) *https://cra.org/wp-content/uploads/2024/07/Report-Conference-Submission-and-Review-Policies.pdf.*

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. EL25–14–000]

Idaho Power Company; Notice of Institution of Section 206 Proceeding and Refund Effective Date

On December 5, 2024, the Commission issued an order in Docket No. EL25–14–000, pursuant to section 206 of the Federal Power Act (FPA), 16 U.S.C. 824e, instituting an investigation to determine whether Idaho Power Company's Rate Schedule is unjust, unreasonable, unduly discriminatory or preferential, or otherwise unlawful. *Idaho Power Company,* 189 FERC ¶ 61,172 (2024).

The refund effective date in Docket No. EL25–14–000, established pursuant to section 206(b) of the FPA, will be the date of publication of this notice in the **Federal Register**.

Any interested person desiring to be heard in Docket No. EL25–14–000 must file a notice of intervention or motion to intervene, as appropriate, with the Federal Energy Regulatory Commission, in accordance with Rule 214 of the Commission's Rules of Practice and Procedure, 18 CFR 385.214 (2023), within 21 days of the date of issuance of the order.

In addition to publishing the full text of this document in the **Federal Register**, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the internet through the Commission's Home Page (*https://www.ferc.gov*) using the ''eLibrary'' link. Enter the docket number excluding the last three digits in the docket number field to access the document. From FERC's Home Page on the internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access