epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

OFFICE OF MANAGEMENT AND BUDGET

Request for Information on Identifying Priority Access or Quality Improvements for Federal Data and Models for Artificial Intelligence Research and Development and Testing

[No. 2019-14618]

August 9, 2019

---

By notice published July 10, 2019, the Office of Management and Budget (OMB) is "inviting the public to identify needs for additional access to, or improvements in the quality of, Federal data and models that would improve the Nation's artificial intelligence (AI) research and development (R&D) and testing efforts."[1] This Request for Information follows from the 2019 Executive Order on Maintaining American Leadership in AI which tasked the OMB director with soliciting public input on the federal data sets and models to be opened for AI.[2]

EPIC supports the public availability of data from the federal government for use in AI research, development, and testing that is not personally identifiable information. From data about climate change to data about the practices of federal agencies, such as disparities in criminal

---

[1] *Identifying Priority Access or Quality Improvements for Federal Data and Models for Artificial Intelligence Research and Development (R&D), and Testing; Request for Information*, 84 Fed. Reg. 32962 (July 10, 2019), https://www.federalregister.gov/documents/2019/07/10/2019-14618/identifying-priority-access-or-quality-improvements-for-federal-data-and-models-for-artificial

[2] Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-americanleadership-artificial-intelligence/.

sentencing, EPIC strongly encourages greater use of government data for learning and analysis. At the same time, EPIC strongly cautions against the use of data sets containing personally identifiable information, noting that federal agencies in possession of personal data are under legal obligations to safeguard that information and also to conduct rulemakings and privacy impact assessments regarding the future of that data. EPIC's view of the use of government data for AI reflects long-standing practices in federal information policy that seek to maximize public access to public information while restricting access to personal data. This is both to promote government oversight and accountability and to ensure fairness for decisions concerning individuals.

EPIC submits these comments to urge OMB to (1) ensure federal agencies make widely available federal data that is not personally identifiable, (2) ensure federal agencies comply with Privacy Act and Section 208 obligations to safeguard personal data in their possession, (3) encourage agencies to comply with framework principles for AI, including the OECD AI Principles and the Universal Guidelines for AI, which both address specific challenges associated with AI techniques and human rights.

**Introduction**

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. [3] In 2014, EPIC launched a campaign for "Algorithmic Transparency" and has subsequently worked with national and international organizations to improve accountability for AI systems.[4] EPIC established the Public Voice project in

[3] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *See, e.g.*, Marc Rotenberg, The Future of Innovation and Digital Transformation: Exploring Societal Impacts, Remarks at the OECD Global Strategic Group Meeting, Epic.org (Nov. 19, 2018), https://epic.org/privacy/ai/Remarks-OECD-CSG-Rotenberg-2018.pdf; EPIC, *At UNESCO, EPIC's Rotenberg Argues for Algorithmic Transparency*, Epic.org, (Dec. 8, 2015), https://epic.org/2015/12/at-unesco-epics-rotenberg-argu.html; EPIC, Algorithmic Transparency

1996 to enable civil society participation in decisions concerning the future of the Internet.[5] And, in 2018, after a petition from EPIC, leading scientific organizations, including AAAS, ACM and IEEE, and nearly100 experts called for public input on U.S. artificial intelligence policy, the National Science Foundation sought public comment.[6] EPIC has also organized public policy panels in both Brussels, Belgium and Washington, DC to bring together experts to address the challenges of AI and to promote the Universal Guidelines for AI.[7]

EPIC has welcomed steps by the White House to include privacy and civil liberties as a centerpiece of the U.S. AI strategy, including U.S. endorsement of the OECD AI Principles.[8] As nations around the world begin to use AI technology to target, profile, track, and influence,[9] strong incorporation of U.S. legal commitments and ethical values in any plan to open U.S. federal data, by contrast, would be another step toward a competitive, long-term vision for AI technology.[10] In this respect, we also support the Administration's desire to desire to advance "American values," though not unique to the United States, which draw a clear distinction between public information and personal data, held by federal agencies.

---

(2018), https://www.epic.org/algorithmic-transparency/; EPIC, *Algorithms in the Criminal Justice System*, epic.org, https://www.epic.org/algorithmic-transparency/crim-justice/.

[5] *See About the Public Voice*, The Public Voice, http://thepublicvoice.org/about-us/.

[6] EPIC, *Following EPIC Petition, National Science Foundation Seeks Public Comment on AI Policy,* Epic.org (Sept. 26, 2016), https://epic.org/2018/09/following-epic-petition-white-.html.

[7] See Public Voice, *The Public Voice: AI, Ethics, and Fundamental Rights, Brussels, Belgium*, Publicvoice.org (Oct. 23, 2018), https://thepublicvoice.org/events/brussels18/; EPIC, *AI and Human Rights: the Future of AI Policy in the US, National Press Club, Washington D.C.*, Epic.org (June 5, 2019) https://www.epic.org/events/June5AIpanel/.

[8] White House, *Artificial Intelligence for the American People*, Whitehouse.gov, https://www.whitehouse.gov/ai/; U.S. Mission to the Org, for Econ. Coop. & Dev., *White House OSTP's Michael Kratsios Keynote on AI Next Step,* Usoecd.usmission.gov (May 21, 2019), https://usoecd.usmission.gov/white-house-ostps-michael-kratsios-keynote-on-ai-next-steps/.

[9] Human Rights Watch, China's Algorithms of Repression (2019), https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.

[10] *See, e.g.*, Comments of EPIC to NIST on "Request for Information on Artificial Intelligence Standards" (May 31, 2019), https://epic.org/privacy/ai/NIST-RFI-EPIC%2020190531.pdf.

## I. The OMB Request for Information

According to the OMB Request for Information:

> The National Artificial Intelligence Research and Development Strategic Plan discusses fundamental challenges, novel ideas for human and AI collaboration, and creating AI that is more trustworthy (e.g., AI techniques that address challenges of bias and fairness, transparency and explainability, and robustness, security, and safety).
>
> Beyond fundamental advances in AI, open challenges also include the application of AI to key domains, such as those highlighted on ai.gov that include:
>
> - Transportation
> - Healthcare
> - Manufacturing
> - Financial Services
> - Agriculture
> - Weather Forecasting
> - National Security & Defense
>
> Depending on the R&D goal and application domain, different data sets and models may be needed to accelerate AI advances. Additionally, the use of these data sets and models could stimulate new developments that would enhance the transparency and explainability of the AI application, and illuminate ways to ensure the robustness, security and safety of AI applications.
>
> Over the years, a number of data sets have already been made available via data.gov. Some of these datasets are fully publicly available, while others have restricted use (see restricted use data sets). However, these data sets may or may not be useful or suitable for AI R&D and testing.
>
> The following lists of topics cover the major areas for which information is sought. These lists are not intended to limit the topics that may be addressed by respondents, who may provide information about any topic that would inform the objective of this action.
>
> To developing requests for additional accesses for data and models to improve AI R&D and testing, input to the following questions is sought:
>
> What Federal data and models are you seeking to use that are available to the public with no use restrictions, but which have technical issues inhibiting data access? Specifically, what are the technical issues (e.g., is it too big to be downloaded, is it not optimally formatted)? What types of AI R&D and testing would be accelerated with increased access to this data?

What Federal data and models are you seeking to use that are restricted to the public, i.e., the data asset is available under certain use restrictions? What types of AI R&D and testing would be accelerated with increased access to this data?

What Federal data and models are you seeking to use that are private and not at all available to the public? Describe the agency that has the data and what, if any, attempts you are aware of that have been made to increase access to the data or model. What types of AI R&D and testing would be accelerated with increased access to this data?

What are key gaps in data and model availability that are slowing progress in AI R&D and testing? Which areas of AI R&D and testing are most impacted?

In developing requests for quality improvements to accessible data and models to improve AI R&D and testing, input to the following questions is sought:

As agencies review their data and models, what are the most important characteristics they should consider? Stated differently, what characteristics of data sets or models make them well-suited for AI R&D?

Which models are most important for agencies to focus on, and why?

What characteristics should the Federal Government consider to increase a data set or model's utility for AI R&D (e.g., documentation, provenance, metadata)?

What data ownership, intellectual property, or data sharing considerations should be included in federally-funded agreements (including, but not limited to, federal contracts and grants) that results in production of data for R&D?

What research questions and applications are you trying to solve with AI, that require specific types and/or quantities of Federal data and models, and how might the Federal Government reduce barriers to discovery and access?

Accelerating the application of AI can be enabled with pre-trained models (e.g., ResNet trained on ImageNet) that facilitate transfer learning. What research questions and applications would benefit most from the transfer learning?

EPIC's comments below respond to several of the questions set out in the OMB Request for Information.

**II. Ensure federal agencies make widely available federal data that is not personally identifiable**

EPIC urges the OMB to center any plan to make available federal data sets on U.S. privacy law and principles for responsible AI. This policy flows naturally from the White House Executive Order on Maintaining American Leadership in Artificial Intelligence, which seeks to "foster public

trust and confidence in AI technologies and protect civil liberties, privacy, and American values."[11] A significant threat to U.S. technology and innovation is user distrust from data misuse, significant breaches, identity theft, overbroad surveillance, and other data driven scandals.[12] However, this history need not be replicated in AI, which can also implicate privacy and data protection interests. Accordingly, any OMB recommendation federal data sets should have a basis in the U.S. Privacy Act and E-Government Act and incorporate the privacy recommendations of the OECD AI principles and Universal Guidelines for Artificial Intelligence.

The Privacy Act of 1974

Any access to personal data held by the federal government for AI R&D must comply with the U.S. Privacy Act of 1974, including provisions on consent for disclosure, public notice, and the exercise of individual rights. The collection, storage, use, or transfer of personal data held by federal agencies is regulated by the Act.[13] At the heart of the Privacy Act is five Fair Information Practices. The FIPs were drafted by the Dep't. of Health, Education and Welfare in response to public outcry over federal data consolidation:[14]

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.

[11] *Id.* § 1(d).
[12] *See, e.g.*, Letter from EPIC to Senate Comm. on Foreign Relations (Mar. 6, 2019) https://epic.org/testimony/congress/EPIC-SFR-KeithKrach-Mar2019.pdf.
[13] Pub. Law 93-579, codified at 5 U.S.C. §552a.
[14] EPIC, *The Code of Fair Information Practices*, Epic.org, http://epic.org/privacy/consumer/code_fair_info.html

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.[15]

Today, the Privacy Act applies these practices systems of records of personal information controlled by federal agencies. The Act requires agencies to provide public notice of systems of records and provides individuals with rights of access and correction.[16] The Act also generally prohibits the disclosure of personal information without consent to "any person, or to another agency" unless an enumerated exception applies.[17]

Section 208 of the E-Government Act

Should federal agencies collect new personal information, obtain new IT or make substantial changes to IT systems for AI R&D, those agencies also must issue a Privacy Impact Assessment in accordance with the E-Government Act of 2002.[18] Section 208 of the Act "ensure[s] sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government."[19] Privacy responsibilities of an agency adhere when developing or procuring new IT, or make a substantial change to existing IT, that collects, maintains, or disseminates information in an identifiable form, or initiates a new collection (defined as obtaining, causing to be obtained, soliciting, or requiring disclosure) of personally identifiable information.[20] An agency is required to conduct, review, and, by default, publish a comprehensive privacy impact assessment *before* obtaining new IT or collecting information.[21] A PIA must address the information to be collected and why, how it will

[15] U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).
[16] 5 U.S.C. § 552a (e)(4).
[17] 5 U.S.C. § 552a(b).
[18] Pub. L. No. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. § 3501 note) (hereinafter "E-Government Act").
[19] E-Government Act § 208(a).
[20] *Id*. at § 208(b)(A).
[21] *Id*. at § 208(b)(B).

be used, any notice or opportunities for consent for individuals, how information will be secured, and whether a system of records is being created under the Privacy Act.[22]

**III. Encourage agencies to comply with framework principles for AI, including the OECD AI Principles and the Universal Guidelines for AI**

OECD Principles on Artificial Intelligence

The OECD Principles on Artificial Intelligence, endorsed by the U.S. government, create new privacy commitments for data driven AI. Announced by the OECD on May 22, 2019 and endorsed forty-two countries, the Principles represent the first international for AI.[23] At the center of the OECD Principles is an aim to "foster innovation and trust in AI by promoting the responsible stewardship of trustworthy AI while ensuring respect for human rights and democratic values."[24] The Principles call for respect for privacy[25] and recommend "a systematic risk management approach" throughout the AI system lifecycle to address risks to privacy and digital security.[26] Importantly, the Principles also encourage governments to open data sets as a matter of national policy, but only to the extent that "privacy and data protection" are respected.[27]

The OECD AI Principles make clear the importance of "human-centered values and fairness." The OECD AI Principles state:

> a)AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labour rights.

---

[22] *Id*. § 208(b)(2)(B)(ii).
[23] Org. for Econ. Co-operation & Dev. [OECD], *Recommendation of the Council on Artificial Intelligence*, C/MIN(2019)3/FINAL (May 22, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [hereinafter OECD Principles on AI].
[24] *See* OECD Principles on AI "Background Information."
[25] *Id*. §1(1.2).
[26] *Id*. §1(1.4)(c).
[27] *Id*. §2(2.1).

> b)To this end, AI actors should implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context and consistent with the state of art.[28]

The OECD AI Principles also underscore the importance of transparency and explainability. Specifically, the OECD AI Principles state:

> AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:
>
> i.to foster a general understanding of AI systems,
>
> ii.to make stakeholders aware of their interactions with AI systems, including in the workplace,
>
> iii.to enable those affected by an AI system to understand the outcome, and,
>
> iv.to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.[29]

The OECD AI Principles seek to promote "robustness, security and safety." As stated in the Principles:

> a)AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk.
>
> b)To this end, AI actors should ensure traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle, to enable analysis of the AI system's outcomes and responses to inquiry, appropriate to the context and consistent with the state of art.
>
> c)AI actors should, based on their roles, the context, and their ability to act, apply a systematic risk management approach to each phase of the AI system lifecycle on a continuous basis to address risks related to AI systems, including privacy, digital security, safety and bias.[30]

The OECD AI Principles also emphasize accountability:

> AI actors should be accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of art.[31]

---

[28] *Id*. §1(1.2).
[29] *Id*. §1(1.3).
[30] *Id*. §1(1.4).
[31] *Id*. §1(1.5).

Finally, the OECD AI Principles also explicitly incorporate the OECD Privacy Guidelines, a widely known privacy framework, which the United States government and U.S. companies have previously endorsed.[32]

Universal Guidelines for AI

EPIC has also recommended the U.S. go further than the OECD AI Principles to adopt the Universal Guidelines for Artificial Intelligence (UGAI) as a basis for U.S. policymaking.[33] A framework of twelve principles designed to safeguard individual rights in the context of automated decision-making, the UGAI was launched in 2018 by the Public Voice Coalition - a global group of civil society organizations.[34] Released in October 2018, over 250 experts and 60 organizations, representing more than 40 countries, endorsed the UGAI.[35] Relevant to access to data sets for AI training, UGAI's "Assessment and Accountability Obligation" requires that AI be "deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks."[36] Corresponding to privacy impact assessment obligation under the E-government Act, if substantial risks to privacy are presented by the use of AI, that use should be forestalled. Similarly, under the "Data Quality Obligation," institutions must limit and record data inputs, establishing "data provenance, and assur[ing] quality and relevance for the data input into algorithms."[37]

**IV. Ensure federal agencies make widely available federal data that is not personally identifiable**

---

[32] *Id*. Preamble.
[33] *See, e.g.*, Comments of EPIC to NIST on "Request for Information on Artificial Intelligence Standards," *supra* note 10.
[34] Public Voice, Universal Guidelines for Artificial Intelligence (2018), https://thepublicvoice.org/ai-universalguidelines/ [hereinafter UGAI]
[35] Public Voice, *Universal Guidelines for Artificial Intelligence: Endorsement*, ThePublicVoice.org, https://thepublicvoice.org/AI-universal-guidelines/endorsement/.
[36] UGAI #5.
[37] UGAI #7.

To simultaneously support U.S. legal obligations and principles for ethical AI *and* advancement AI R&D and testing, OMB should prioritize access to non-personal data sets for AI research. In particular, anonymized or aggregate data gathered from personal data or data which poses no privacy risks at all represent ideal data sets for AI training. Notably, even while strictly regulating the processing of personal data under the GDPR, the EU has encouraged the use of this non-personal data for AI training purposes.[38] The U.S. should follow a similar approach. Nonetheless, OMB must be cognizant that technological advances make re-identification of anonymized data more feasible, and should employ privacy preserving techniques like data minimization and good security hygiene to mitigate any remaining privacy risks.

Aggregate and effectively anonymized data sets are a strong resource for AI training that does not implicate the same privacy risks as personal data sets. Indeed, non-personal data extracted from sensitive personal data sets have long provided significant insights on the activities of government. The U.S. wiretapping reports have long followed this approach:

> Remarkably, in the privacy field some of the most sensitive data in government is made available to the public. For almost 50 years the Administrative Office of the United States Courts has provided detailed reports on the use of surveillance authority in the U.S. Those reports document the use of wiretapping by the federal government—its frequency, cost, reasons for use (most wiretaps concern drug investigations not terrorism) and effectiveness. The data makes possible meaningful oversight of law enforcement activities. And even when law enforcement agencies and civil liberties advocates debate the scope of government surveillance, there is a common data set that informs the discussion.[39]

This data is regularly made available without compromising investigations, revealing the names, or other sensitive details concerning individuals.[40] Indeed, the report is considered a gold standard in

---

[38] *See, e.g.*, Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018 O.J. (L. 303) 59.

[39] Marc Rotenberg, *Let's Use Government Data to Make Better Policy*, Sci. Am. (Oct. 4, 2017), https://blogs.scientificamerican.com/observations/let-rsquo-s-use-government-data-to-make-better-policy/.

[40] *Id*.

U.S. oversight of electronic surveillance authority.[41] Similarly, statistical data quantifying number, category, and types of complaints issued to a federal agency could provide valuable insights into how a federal agency addresses public concerns. For example, in response to an EPIC FOIA request, the FTC was able to confirm a total of 26,000 pending consumer complaints at the agency concerning Facebook, and a breakdown of complaints per year.[42] While individual consumer complaints inherently contain personal data, de-identified aggregate statistical information reveal information about how federal resources are used and improve agency accountability.

Other government data sets are fundamentally composed of non-personal data and pose no privacy threat. The National Oceanic and Atmospheric administration tracks hurricanes across the Atlantic, forecasting which has improved significantly over a century.[43] Officials around the country rely on such data "to make difficult decisions about how to deploy resources and when to evacuate residents of coastal communities."[44] Similarly, in the context of industrial farming "data on precision farming... can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines" can be used to improve efficiency.[45]

Nonetheless, OMB should be cognizant that technological advances increasingly drawing connections between data points otherwise invisible from human review, rendering some non-personal data personal. Where privacy risks are unavoidable, agencies must rely on additional privacy protective techniques like data minimization and good security hygiene when providing access to data

[41] EPIC, *Wiretapping*, Epic.org, https://epic.org/privacy/wiretap/.
[42] EPIC, *EPIC FOIA - FTC Confirms Number of Pending Facebook Complaints, Doubling Every Two Years*, Epic.org (Apr. 3, 2019), https://epic.org/2019/04/epic-foia---ftc-confirms-numbe.html.
[43] Marc Rotenberg, *supra* note 39.
[44] *Id*.
[45] Regulation (EU) 2018/1807, 2018 O.J. (L. 303) 59, 60.

for AI purposes. In 2017, the National Academies of Sciences, Engineering, and Medicine recently completed two studies on this topic.[46] the National Academies concluded:

> Threats from data breaches and the growing availability of other sources of data that might be used to re-identify individuals or entities require statistical agencies to reconsider how they can maintain data confidentiality. The publication of statistics covering various groups and subgroups requires careful consideration of how to safely release statistical products and of the potential privacy losses that might occur… there are fundamental mathematical limits on 'how much' can be computed while maintaining any reasonable notation of privacy: extremely detailed estimates of too many statistics can effectively result in a complete loss of privacy.[47]

The report identifies specific tools to address unavoidable privacy risks: "minimizing the personal data that are collected, minimizing disclosure risk by restricting the data that are released, controlling access to and use of the data, encrypting data, and using differential privacy techniques to measure and control cumulative privacy loss."[48] Agencies should rely on these privacy protective techniques where granting access to personal data or where non-personal data risks identification.

**V. Conclusion**

EPIC recommends any plan to open federal data for AI R&D and testing rigorously incorporate U.S. privacy law, such as the Privacy Act and E-Government Act Section 208, as well as principles for responsible AI. Toward this goal, EPIC encourages the OMB to prioritize relying on non-personal data sets for the advancement of AI, and rely on privacy protective techniques to minimize privacy risks where privacy is implicated.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

---

[46] *See* Nat'l Acad. of Sci., Eng'g, & Med., Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy 82 (2017). See also Nat'l Acad. of Sci., Eng'g, & Med., Federal Statistics, Multiple Data Sources, and Privacy Protection: Next Steps (2017).
[47] Nat'l Acad. of Sci., Eng'g, & Med., Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy at 82, 92.
[48] *Id*. at 82.

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC International Counsel

*Legal Scholars and Technology Experts*

Francesca Bignami, Professor of Law, The George Washington University Law School
Christine L. Borgman, Distinguished Professor & Presidential Chair in Information Studies, UCLA
Danielle Keats Citron, Morton & Sophia Macht Professor of Law, University of Maryland Francis King Carey School of Law
David J. Farber, Adjunct Professor of Internet Studies, Carnegie Mellon University
Addison Fischer, Founder and Chairman, Fischer International Corp.
David Harris Flaherty, Former Information and Privacy Commissioner for British Columbia
Jerry Kang, Vice Chancellor for Equity, Diversity and Inclusion, UCLA
Len Kennedy, EPIC Scholar in Residence
Lorraine Kisselburgh, Chair, Association for Computing Machinery Tech Policy Council
Harry R. Lewis, Gordon McKay Professor of Computer Science, Harvard University
Chris Larsen, Executive Chairman, Ripple Inc.
Roger McNamee, Co-Founder, Elevation Partners
Pablo Garcia Molina, Adjunct Professor, Georgetown University
Erin Murphy, Professor of Law, NYU School of Law
Peter G. Neumann, Chief Scientist, SRI International Computer Science Lab
Helen Nissenbaum, Cornell Tech, Professor, Information Science
Frank Pasquale, Professor of Law, Univ. of Maryland Francis King Carey School of Law
Deborah C. Peel, M.D., President of Patient Privacy Rights
Stephanie Perrin, President, Digital Discretion, Inc.
Bilyana Petkova, Assistant Professor, Department of International and European Law, Maastricht University
Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School
Professor Sherry Turkle, Abby Rockefeller Mauz_ Professor of the Social Studies of Science and Technology, MIT
Nadine Strossen, John Marshall Harlan II Professor of Law, New York Law School
Ari Waldman, Professor of Law, Director of the Innovation Center for Law and Technology, New York Law School.
Jim Waldo, Gordon McKay Professor of the Practice of Computer Science, John A. Paulson School of Engineering and Applied Science
Ann L. Washington, Assistant Professor of Data Policy, NYU Steinhardt School; Visiting Scholar Data & Society Research Institute
Christopher Wolf, Board Chair, Future of Privacy Forum
Shoshana Zuboff, Charles Edward Wilson Professor of Business Administration, Harvard Business School