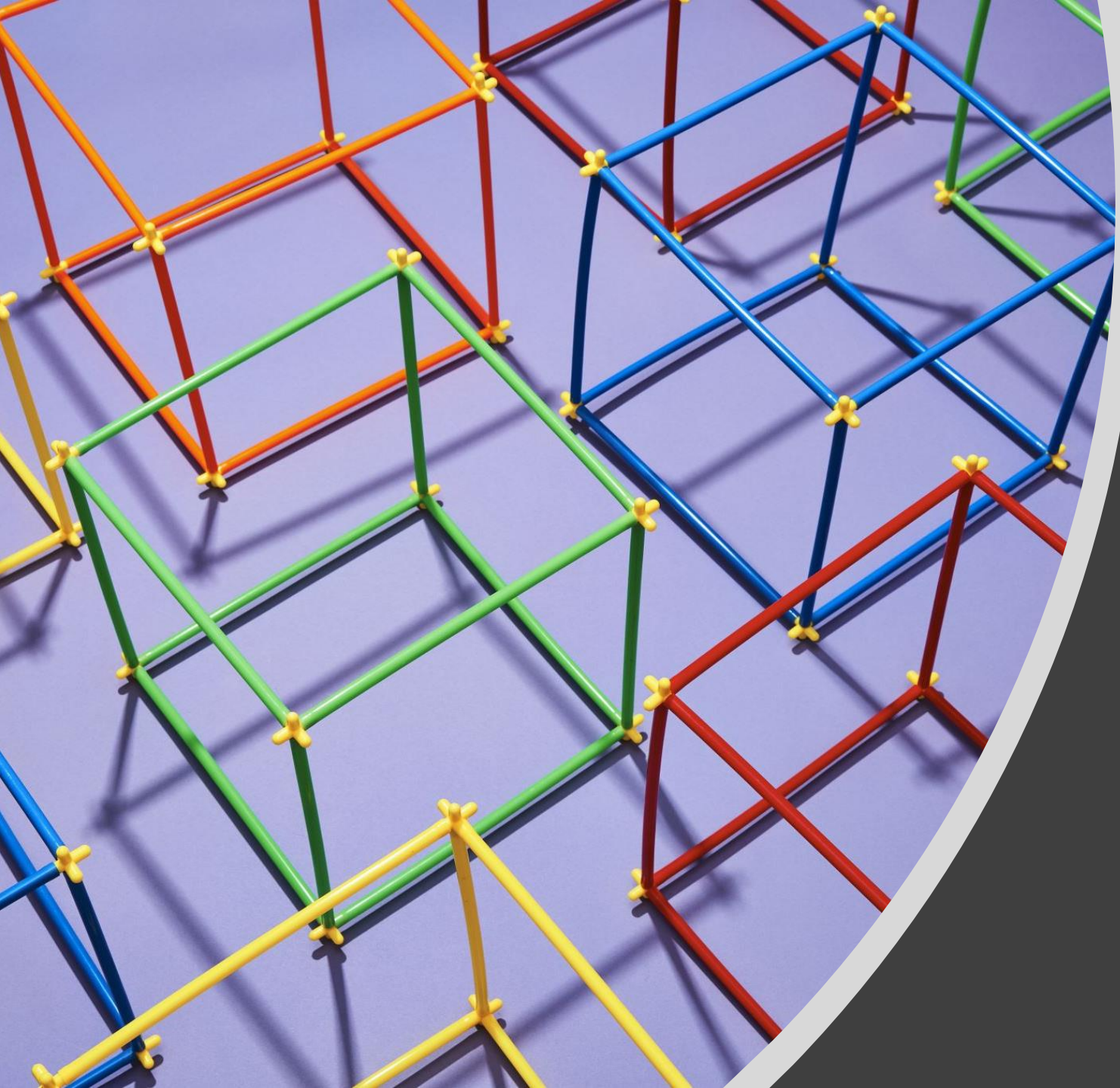


Evolving Ethics of Data Sharing

Professor Anita L. Allen, JD, PhD

Henry R. Silverman Professor of Law and Professor of Philosophy

University of Pennsylvania Carey Law School

NEW NIH Data Management and Sharing Policy

- AIM:

"promote the management and sharing of scientific data generated from NIH-funded or conducted research."

Questions

What values should regulators and researchers have in mind as they seek to expand access to research?

Will the fair enforcement of the new policy be more challenging due to its flexible standards?

Who is intended to benefit from the new rules? Who will in fact benefit?

Does an emphasis on reducing barriers and increasing incentives place the data of vulnerable populations greater at risk of wrongful disclosure?

How can researchers ethically ….

- collect and document data;
- possess, use and own data
- secure, share, publish disclose data/sensitive data;
- comply with legal and agency implementation of policy (e.g., HIPAA, Common Rule, CC's, NIH policies);
- meet responsibilities owed public implicit in public funding for research?

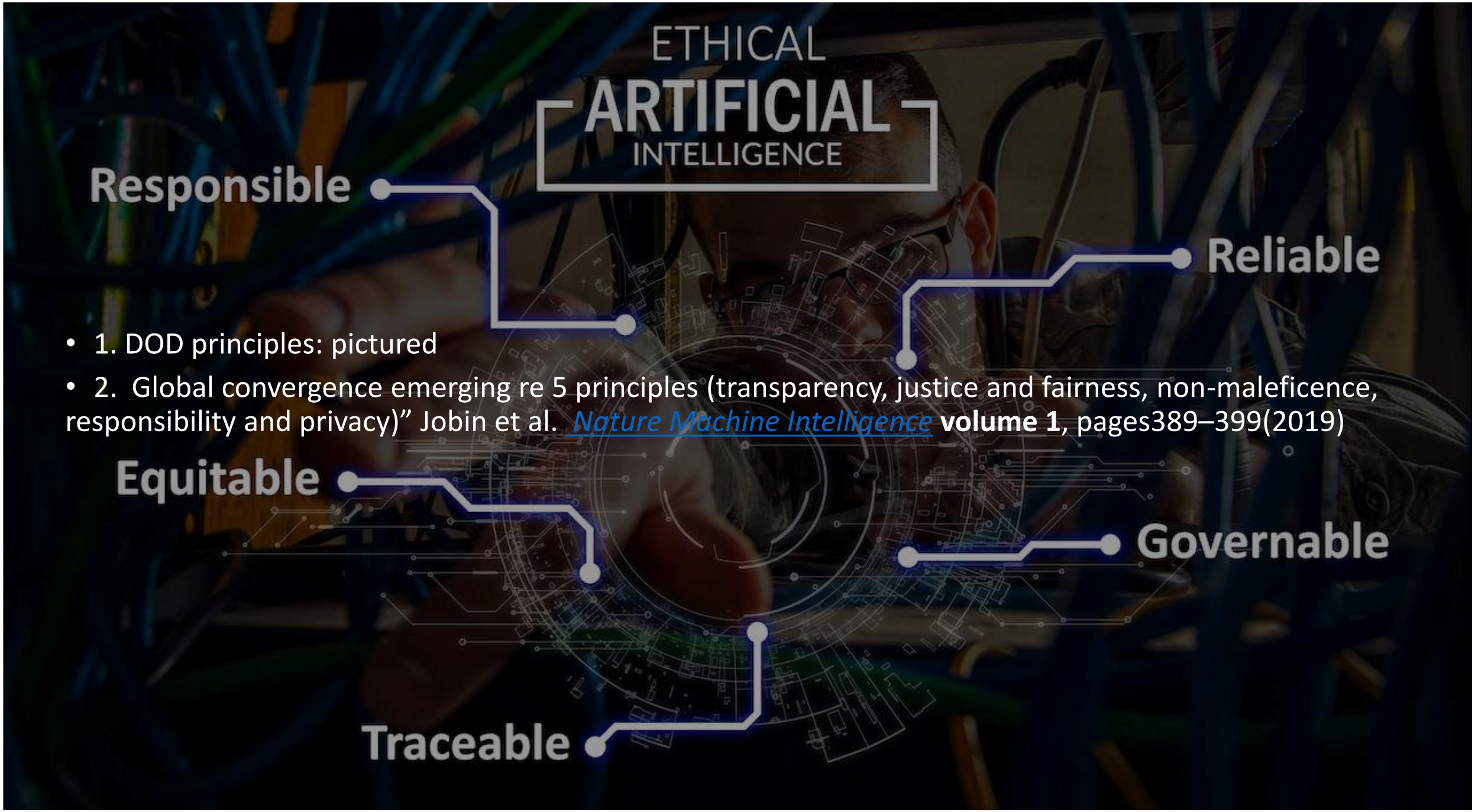
Promote Autonomy, Dignity and Welfare through "Fair Information Practice Principles"

- "FIPs began in the 1970s with a report from the Department of Health, Education & Welfare.
- The Organization for Economic Cooperation and Development revised the principles in a document that became influential internationally.
- FIPs have evolved over time, with different formulations coming from different countries and different sources over the decades.
- FIPs are increasingly recognized today as part of international privacy policy discussions, standards, and laws. Many today consider FIPs to be necessary but not sufficient as privacy standards."
- Robert Gellman (updated 2021) https://bobgellman.com/rg-docs/rg-FIPShistory.pdf

FIPs

(International Association of Privacy Professionals Version)

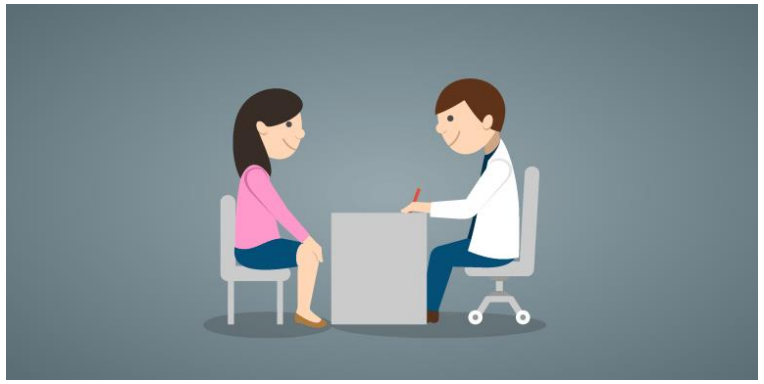
- (1) **The Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
(2) **The Data Quality Principle.** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
(3) **The Purpose Specification Principle.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
(4) **The Use Limitation Principle.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except a) with the consent of the data subject, or b) by the authority of law.
-
(5) **The Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
(6) **The Openness Principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
(7) **The Individual Participation Principle.** An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have data relating to him communicated to him, within a reasonable time, at a charge, if any, that is not excessive; in a reasonable manner, and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;
(8) **The Accountability Principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.
-



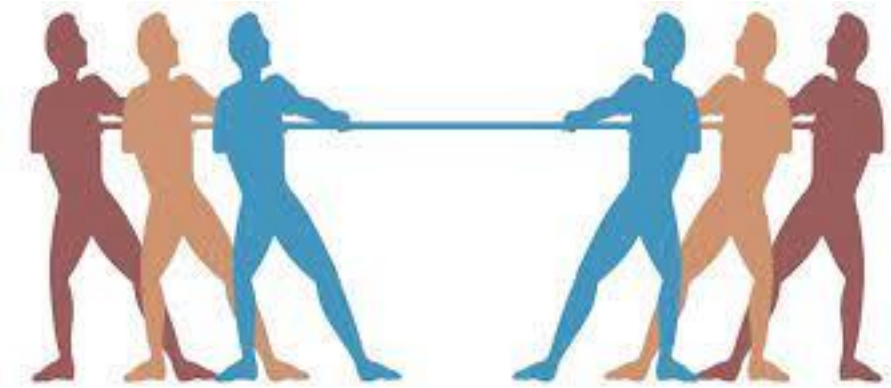
- 1. DOD principles: pictured
- 2. Global convergence emerging re 5 principles (transparency, justice and fairness, non-maleficence, responsibility and privacy)" Jobin et al. *Nature Machine Intelligence* **volume 1**, pages389–399(2019)

Challenge: Ethics of Professional Data Collection and Sharing Research Compete with the Ethics of Self-Disclosure

- Data Management: Professional Ethics



- Data Self-Management: Self-Care and Care for Others; Duties to Self



Subjects may decline research when well-informed about legal rights…so?

- Finding: When given both informed consent and HIPAA authorization, a lower percentage of African American subjects were willing to be involved in a hypothetical anti-hypertensive medication research study, than subjects in a control group only given informed consent
- Citation: A. Dunlop et al. The Impact of HIPAA Authorization on Willingness to Participate in Clinical Research. November 2007. Annals of Epidemiology 17(11):899-905

FIGHT BIAS-- RESPECT ALL CULTURES

- The University of Pennsylvania apologized to members of MOVE on Monday for using the remains of one of the group's members as a case study in its anthropology classes, rather than returning them to the family.
- "We understand the importance of reuniting the remains with the family and we are working now to find a respectful, consultative resolution," a university spokesperson said. "... We are reassessing our practices of collecting, stewarding, displaying, and researching human remains."

Conclusion

- In addition to traditional bioethical principles, promulgate digital-era specific information management principles.
- Exercise administrative discretion implicit in the new policy judiciously and fairly.
- Train against biases that obscure and undervalue the data interests of vulnerable populations and cultures affected by research sharing.