Governing Ethical AI in ICICLE

Sadia Khan (Indiana University)
Beth Plale (Indiana University)
Neelima Savardekar (The Ohio State University)
Alfonso Morales (University of Wisconsin)

Conference on Ethical and Responsible Design in the National AI Institutes

Georgia Institute of Technology, May 10-12, 2023

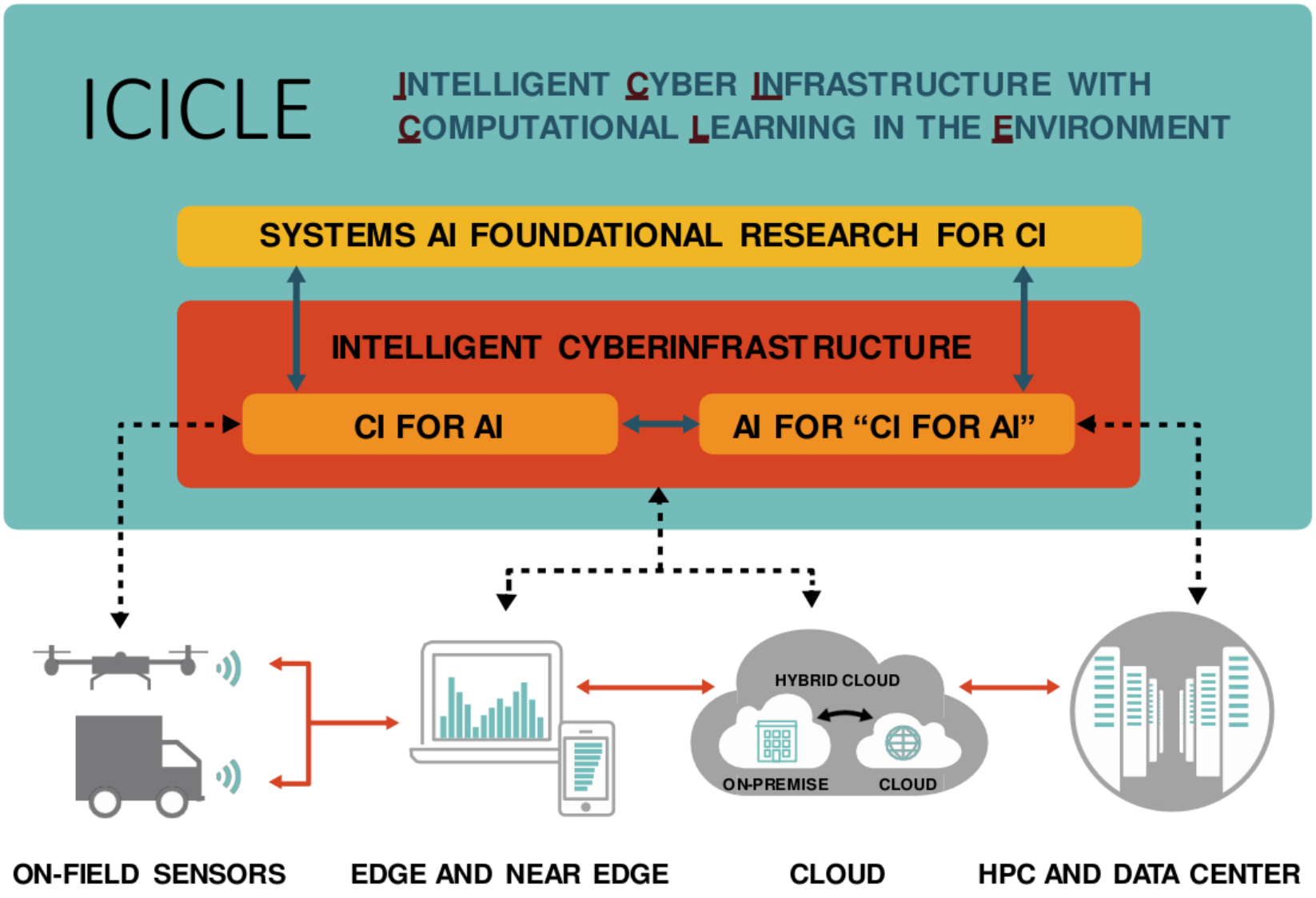
PERVASIVE TECHNOLOGY INSTITUTE

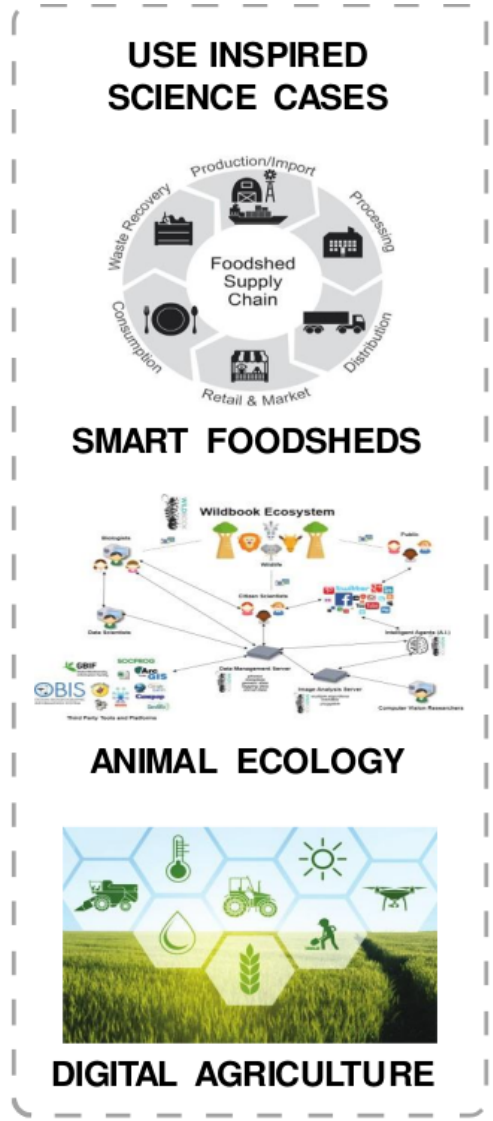
Intelligent Cyberinfrastructure with Computational Learning in the Environment (ICICLE)

National infrastructure that enabling AI use-inspired research and practice at the flick of a switch

- US National Science Foundation Funded AI Institute
- http://icicle.ai
- Award # 2112606

ICICLE in a nutshell



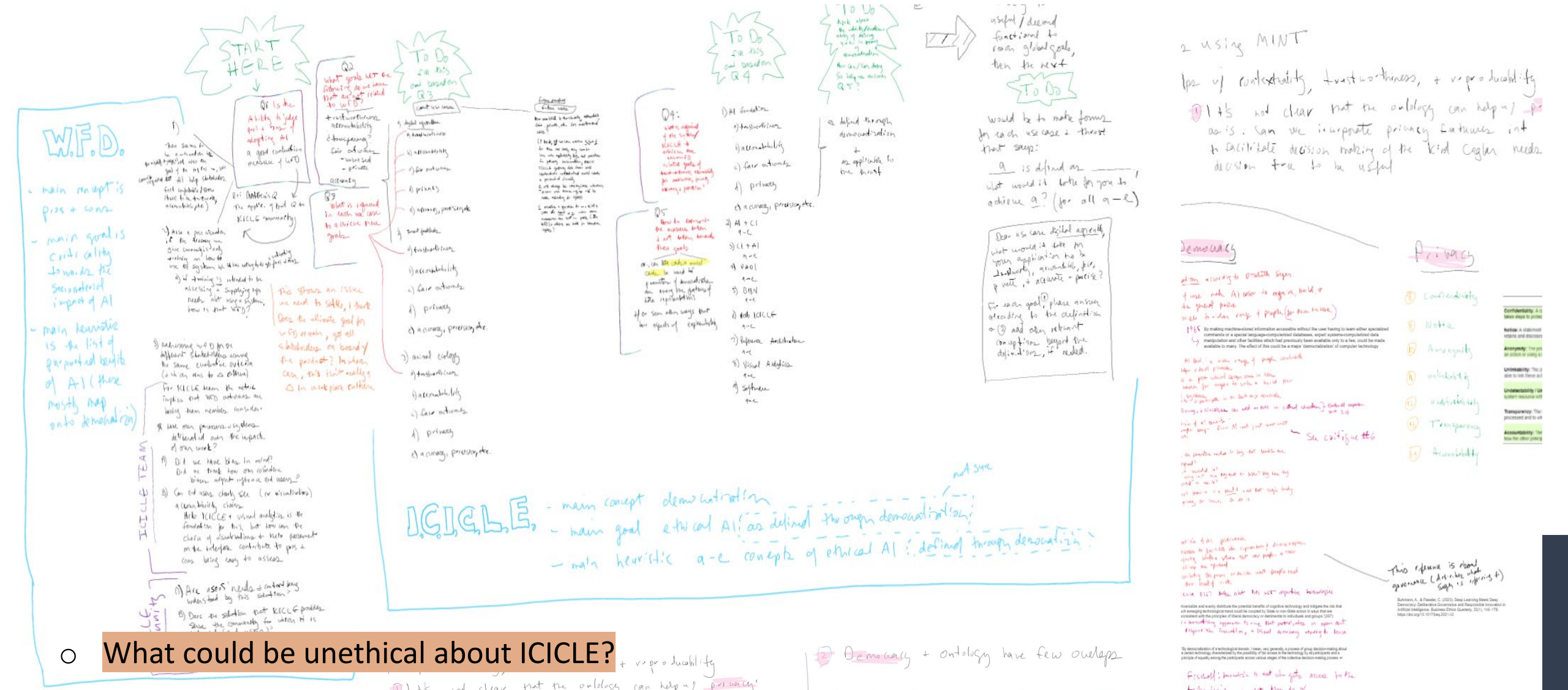


Democratizing AI is a tagline of ICICLE.

Democratizing AI is a tagline of ICICLE.

Ethical development is an imperative

- What could be unethical about ICICLE?
- What do we about it?
- How do we evaluate *if* and ensure *that* "ethics" and "democratization" have been accomplished?



- What could be unethical about ICICLE?
- What do we about it?
- How do we evaluate *if* and ensure *that* "ethics" and "democratization" have been accomplished?

The twin challenges of developing *ethical* and *democratic AI*.

The ICICLE AI Ethics working group worked through a framework for how to operationalize democratization in a way that has impact on the team, its work, and the current and future stakeholders who will use ICICLE cyberinfrastructure

ICICLE Ethics Statement

Developed by a consortium of researchers, educators, and community leaders from Artificial Intelligence (AI), cyberinfrastructure (CI), and food systems, precision agriculture, and animal ecology domains across thirteen institutions, ICICLE employs an edge-to-center, plug and play model that builds trustworthiness into the system by leveraging domain knowledge to facilitate contextual, sustainable, and democratizing outcomes. Democratizing AI demands not only equitable access, but trustworthiness in practice and research. This is performed at ICICLE's ***Institutional Level*** through team-wide workforce development training activities in unconscious bias and bias in data and models; through the implementation of a project-wide, auditable (transparent and reproducible) workflows; and through the co-design of field edge-to-HPC/Cloud infrastructure. And, it is executed at the ***AI/System Level*** through data integrity and privacy preserving practices, and through an ontology-driven system architecture focused on traceable, conversational, and graphical explainability.

Steps to operationalization

1.

Democratizing AI benefits and development

through workforce training in ethics and allyship

Centering ICICLE design within the landscape of ethics:

Resurfacing historical, ethical concerns

(STS and Information Theory)

Drawing on contemporary work on AI ethics

(participating in the discourse on FAIR /FACT and ethical AI)

Bringing real world issues of bias and social harm into focus

(thinking about stakeholders in the context of the risks of AI)

Dimensions of Privacy

- Public/Private Disclosure of Facts — Prosser (1960)
- Right to be Let Alone — Warren and Brandeis (1890)
- Intrusion Upon Seclusion — Prosser (1960)
- False Light — Prosser (1960)

- Dignity/Self Representation
- Consent/Autonomy
- Power/Control

Prosser, W. (1960). *Privacy*, 48 CALIFORNIA LAW REVIEW 383. (Prosser divided privacy into four tortious acts.)
Warren, S. D., & Brandeis, L. (1890). Warren & Brandeis, The Right to Privacy, 4 HARV. L. Rv. 193 (1890). *Harvard Law Review*, *4*(5), 193.

Cameras and drones can capture and affect more than a specific object of interest.

Drones and other surveillance technologies are "contested objects" that mediate behaviors, access, and movement of human and non-human beings, based on who feels safe being seen (Parks and Kaplan 2017).

Michael Williams sat behind bars for accused murder for nearly a year based on a facial recognition match from a surveillance camera before the evidence was **deemed inaccurate** (Burke, et al. 2022).

Individuals can be reidentified and their sensitive information exposed with minimal personal information.

"In many cases … the database itself depends on the data holder's ability to produce anonymous data because not releasing such information at all may diminish the need for the data, while … **failing to provide proper protection within a release may create circumstances that harm the public or others**" (Sweeney, L. 2002).

1. *Life in the Age of Drone Warfare*, edited by Lisa Parks, and Caren Kaplan, Duke University Press, 2017.
2. Grewal, I. (2017). DRONE IMAGINARIES. The Technopolitics of Visuality in Postcolony and Empire. In *Life in the Age of Drone Warfare* (pp. 343-366). Duke University Press.
3. Burke, et al. *How AI-powered tech landed man in jail with scant evidence*. (2021, August 19). AP NEWS. https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220
4. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International journal of uncertainty, fuzziness and knowledge-based systems*, *10*(05), 557-570.

Tip 1: Be **transparent** and **thorough in documentation** about ownership, data retention and availability, portability, and the like.

- Transparency helps others evaluate tradeoffs.
- Documentation is necessary to activate access control.

"How do we do it"?

Resurfacing historical, ethical concerns
(STS and Information Theory)

Bringing contemporary, real-world issues of bias and social harm into focus
(thinking about stakeholders in the context of the risks of AI)

Drawing on current work on AI ethics
(participating in the discourse on FAIR and ethical AI)

I. Workforce Development
- A. *challenge inevitability*…
- B. *encourage forethought*…

II. DEI and BPC (*democratization of AI devt.* to help minimize bias

Let's build a workforce that considers ethical implications!

III. Democratization
- A. *Engage end-users* to maximize accessibility & minimize risk

IV. Trustworthiness
- A. Use *model cards* to build trust through accountability and contextuality)

Let's focus on stakeholders and use-inspired science!

V. Privacy
- A. Employ privacy preserving techniques (requires *transparency* and *documentation*)
- B. Apply *contextual integrity*/evaluate privacy tradeoff

VI. Fairness

VII. Accountability (accountable to & accountable for)
- A. Governance and reporting
- B. Utilize KG & visual analytics with *FAIR/FACT principles*

Let's harness the best methods in privacy, accountability, transparency, and more!

Other Steps

2. Employing model cards as a mechanism to built trust through accountability and contextuality.

Method

MODEL CARDS: a mechanism for improving accountability in AI/ML development [5]

- Model cards offer a standardized method of documentation for model building which encourages transparent model reporting
- Model card reporting requires model developers to specify the context in which models are intended to be used, the performance statistics on a variety of conditions (such as cultural, demographic, and phenotypic groups), and other relevant information

Ontology Foundry

- drawing on ontology from SDO, PPOD and etc,.
- Ontology components:
  - MINT Model ontology
    - process
    - input variables
    - output variables
    - …
  - Privacy
    - ownership
    - copyrightHolder
    - conditionsOfAccess
    - …
  - FAIR / Transparency
    - downloadURL
    - documentationURL
    - installation instructions URL
    - …
  - Trustworthiness
    - citation
    - license
    - …

3.

Broadening impacts of the democratization of AI development via the development of ethics tips appropriate for high schoolers.

4.

Outreach and stakeholder involvement to democratize AI use—operationalized through an educational fellows program.

*The National Science Foundation-funded AI Institute for Intelligent Cyberinfrastructure with Computational Learning in the Environment (**ICICLE**) is now accepting applications for its **2023 Educational Fellows Program**.*

5.

Democratization of AI benefits through use-inspired science via implementation of stakeholder privacy concerns.

“Farmers must share information about the environmental conditions and the soil conditions of their farms in order to participate in many programs. The risks that they take include adverse pricing and competitive disadvantages as well as price discrimination, interference of potential diseases, insurance costs, and farmers interactions. …

The primary technique for securing the privacy of farmers that is offered by adding ‘noise’ to the publicly available information. The effect of the added noise is a calculatable measurement of privacy called epsilon differential privacy. “

Challenges

1. Democratization and ethics are difficult when we don't know who will access ICICLE cyberinfrastructure and how it will impact them.
2. We do not have a lot of contributed data yet to help us anticipate the range of ethical issues. (This is something other institutes could perhaps help us with.)
3. The ICICLE workflow is conducted in thrusts, which naturally creates a siloing effect.
4. There must be some middle ground between starting from scratch with defining ethics and developing a framework and utilizing a broiler-plate governance framework.

Thank you!

Sadia Khan (khanso@iu.edu)

Beth Plale (plale@indiana.edu)

Neelima Savardekar (savardekar.2@osu.edu)

Alfonso Morales (morales1@wisc.edu)

http://icicle.ai