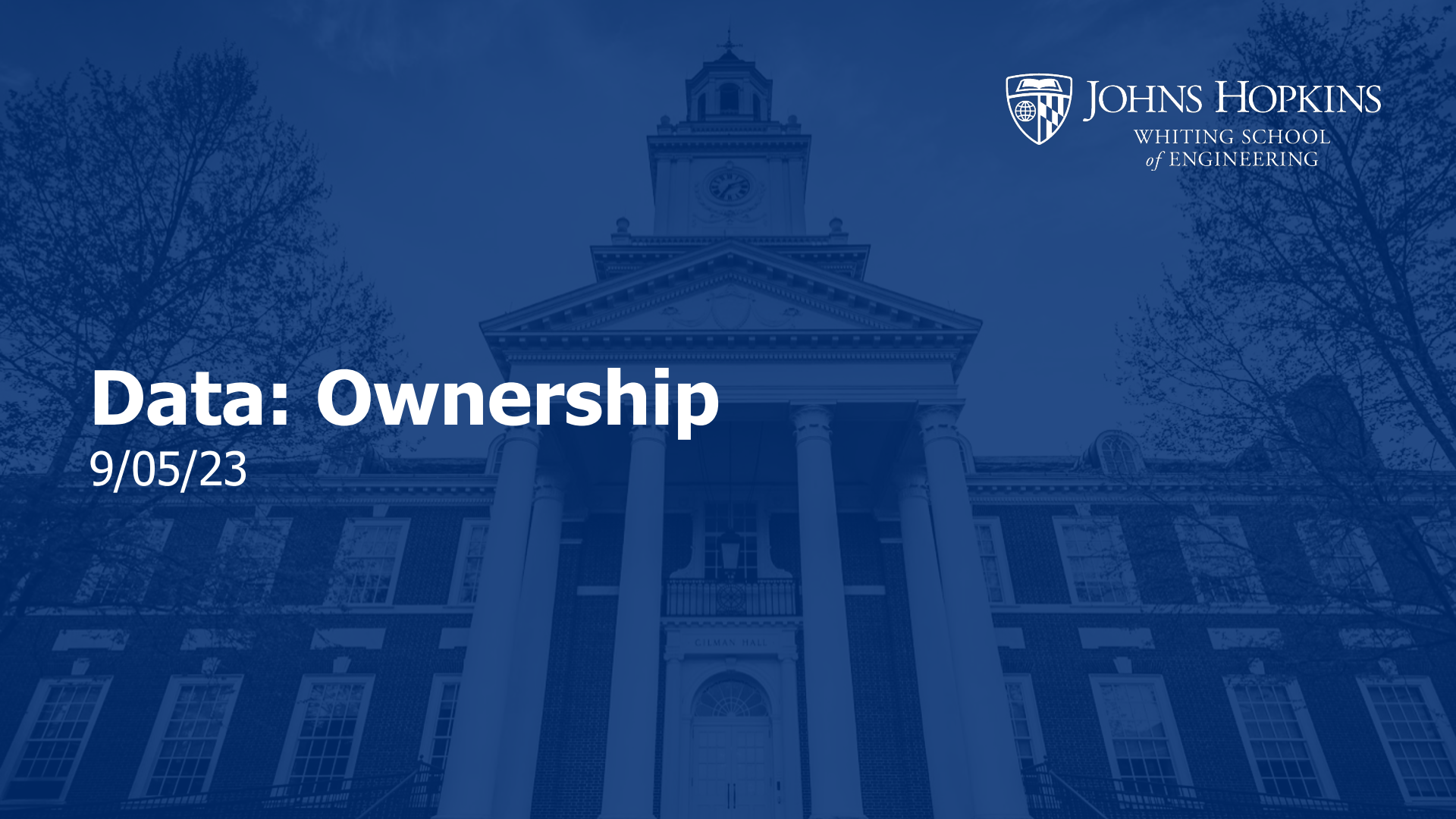

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Data: Ownership

9/05/23

Discussion Groups

- Make sure that each person in your group is talking. If someone is talking less, find a way to draw them in. This is one of the most important parts of your role as facilitator: do your best to have everyone talk (very roughly) the same amount.
- Try not to respond to every comment that everyone makes at your table; instead if no one is talking ask the table what they think about what has just been said. If it feels like the right time to summarize responses, maybe do so without taking a stand one way or another.
- If you need an icebreaker, you might ask a question for which there is no single correct answer and go around the table with it. (Example: "On a scale of 1 to 10, how successful do you think the paper is at solving the problem they pose" or "If you were going to do a project following up on this paper, which part of the paper might be most rewarding to look into?")
- Try to be careful about giving credit for ideas

Class recap

- Share 3 specific takeaways from the discussion:
  - "We were surprised by…"
  - "We couldn't agree on…"
  - "We came up with these recommendations for how to…"

- **Not** intended to be a summary of the entire discussion, instead, it should be the **outcomes** of your discussion

Brief History of Facial Recognition Research

- 1960s: Woody Bledsoe, Helen Chan Wolf, and Charles Bisson try to get computers to recognize faces
- 1993-1996: DARPA FERET project
  - "to develop automatic face recognition capabilities that could be employed to assist security, intelligence, and law enforcement personnel in the performance of their duties"
- 1996-2006: FERET dataset simulates research interest, but models are not very good
- 2007-2013: Mainstream development for unconstrained settings
  - Hunt for "in the wild data sets"
- 2014-present: Deep learning leads to more accurate models and commercialization

https://www.nist.gov/programs-projects/face-recognition-technology-feret

Raji, Inioluwa Deborah, and Genevieve Fried. "About face: A survey of facial recognition evaluation." AAAI 2020 Workshop on AI Evaluation (2021).

How is facial recognition technology used?

Ad from a face image processing company

> "We live in a dangerous world, where harm doers and criminals easily mingle with the general population; the vast majority of them are unknown to the authorities….Public Safety agencies, city police department, smart city service providers and other law enforcement entities are increasingly strive for Predictive Screening solutions, that can monitor, prevent, and forecast criminal events and public disorder without direct investigation or innocent people interrogations.

> "What if it was possible to know whether an individual is a potential pedophile, an aggressive person, or a criminal?"

How is facial recognition technology used?

- Emotion expression and intensity
- Sexual orientation
- Political orientation
- Personality traits

A large body of work in psychology and anthropology has provided evidence that "there is no relationship between how we look and how trustworthy or intelligent we actually are", though opposing research exists

Severin Engelmann, Chiara Ullstein, Orestis Papakyriakopoulos, and Jens Grossklags. 2022. What People Think AI Should Infer From Faces. (FAccT '22) https://doi.org/10.1145/3531146.3533080

Where is facial recognition technology not used?

2018:

- Intense criticism of facial recognition research as surveillance tech (petitions, letter to Jeff Bezos)
- Gender Shades Project

2020:

- Amazon places 1-year moratorium on use of it's face-processing software by police agencies (which they extended at least one more year)
- Microsoft stops selling facial-recognition software to police
- IBM halts work on face recognition because it's used for racial profiling

https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/
https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/
https://www.technologyreview.com/2020/06/09/1002947/ibm-says-it-is-no-longer-working-on-face-recognition-because-its-used-for-racial-profiling/

NIST Evaluation Program

- https://www.nist.gov/programs-projects/face-projects

Face Recognition Technology Evaluation (FRTE) 1:1 Verification

Latest Report | Participation Agreement | API | Validation | Encryption | Submit

▾ Status

[2024-08-09] A new FRTE 1:1 report has been published.

[2024-07-03] NIST included all algorithms evaluated since the ongoing FRTE evaluation started in 2017. Previously we listed only results for each developer's two most recent implementations. This change allows end-users to reference results for algorithms that have been superseded by newer variants, but which may still be used operationally. We added a "by developer" tab which lists only the most accurate algorithm from each developer, where accuracy is defined by the lowest FNMR value for the visa-border dataset.

Credit: Natasha Hanacek/NIST

[2024-03-27] NIST discontinued running the FRTE Visa-Visa benchmark on 1:1 algorithms submitted to FRTE.

[2023-07-03] All algorithms, participation agreements, and GPG keys should be submitted using the FRTE Submission Form.

Except PAD, all FRTE tracks are open. Algorithms submitted to the FRTE 1:1 track will be run on all the datasets documented in the FRTE 1:1 report.

Next: Data Privacy

1. Carlini, Nicolas, et al. "Extracting training data from diffusion models." 32nd USENIX Security Symposium (USENIX Security 23). 2023.
2. Hannah Brown, Katherine Lee, Fatemehsadat Mireshghalla, Reza Shokri, Florian Tramèr. "What Does it Mean for a Language Model to Preserve Privacy?" FAccT 2022.

Fill out course goals form by Tuesday 9/10!

- https://forms.office.com/r/SjMWteg65e