## Do you have the users' consent to Privacy Enhancing Technologies collect and process their information or did you forget to get consent? Decision Tree Are you sharing information with a 3rd Go get consent or party or directly with the user or forget about it. group of users whose data you are making predictions on? Do you have to share insights or share Can predictions be done on user a dataset that needs to be visible? devices or do you have to collect the data in a central database? Are you making generalizations over a Do you need personally identifiable population or user-specific information to be in the dataset (e.g., Do you only want to predict or do you Do you need personally identifiable names, social insurance numbers, predictions? want to train a model based on the information to be in the dataset (e.g., users' data? faces) or can the data be useful names, social insurance numbers, faces) or can the data be useful without it? without it? Are you training a machine learning Do the outputs have to be kept secret from you or can you view them? model or answering queries made to a Optimize model for speed Federated Learning using database? differentially private gradient Have a Data Processing Agreement, Are you dealing with and size and deploy on the Encryption in Are you dealing with structured (pre-defined encrypt in transit, and keep track of edge (e.g., cell phone, descent, with secure structured (pre-defined transit and at rest, who you shared the prediction with format) or unstructured multiparty computation for browser, etc.). Strict access format) or unstructured (e.g., text, images, video, and what it is being used for. model update aggregation. (e.g., text, images, video, controls. speech) data? Potentially good candidate for speech) data? Secure Multiparty Computation. Is/are the other party/parties Is latency a critical Differentially Private Differential Privacy contributing sensitive input requirement or can Training (e.g., differentially computations take a little data or can you compute the private gradient descent) or output without additional longer and be approximated training on pseudonymized sensitive information? using polynomial operations? or synthetic data. Data aggregation + differential Risk-based data de-identification Data aggregation + differential Risk-based data deprivacy or risk-based data deand/or data synthesis using Al. privacy or risk-based data deidentification and/or data identification and/or data synthesis. identification and/or data synthesis. synthesis using Al. Encryption in transit and at rest, Strict access controls. Encryption in transit and at rest, Encryption in transit and at Encryption in transit and at rest, Homomorphic De-Identification, Data Trusted Execution Can you afford higher Strict access controls. Strict access controls. rest, Strict access controls. Environments (e.g., Intel SGX, Encryption communication costs and Processing Agreement,

have repeatable algorithms

to run or not?

Secure Multiparty

Computation

Keybase)

Encryption in transit

and at rest, Strict

access controls.

Data Processing Agreement,

Encryption in transit and at

rest, Strict access controls.

