B.4: Talking Points — Tips on language and privacy lingo

General language tips

- **Use terms your audience will understand.** Unless you have a particularly sophisticated room of experts, avoid technical jargon and translate these concepts into terms your stakeholders might use themselves. Be creative when attempting to distill complicated concepts: use metaphors, visuals, and hypotheticals; practice breaking ideas down and explaining them to a friend or family member, a 5-year-old[23], or a rubber duck[24]; or use tools like the UpGoer 5 Generator[25], the Sideways Dictionary[26], or another Data Glossary[27].

- **Use AISP's resources** on "What is an IDS" and "What is administrative data" to create a consistent vocabulary, and pay attention to how your peer organizations are messaging their work[28].

- **Pay attention to other campaigns** supporting evidence-based policymaking at the local, state, and federal level. Observing these efforts can help you identify potential collaborators, hot button issues, and examples of successful (or unsuccessful) messaging.

Privacy lingo and common pitfalls

- **Anonymous.** To many of those deeply invested in advanced technical privacy protections, "anonymous" is a fighting word. Using it can trigger a debate about when data can be legally or scientifically described as anonymous, which will distract from your broader message[29]. When speaking to *disclosure control, privacy and data science experts*, try not to describe data as "*anonymous*" if it can be more precisely defined as "de-identified according to agreed-upon standards," "aggregated," "hashed," etc.[30] When speaking to *lay audiences* and *policymakers*, it may be appropriate to use "anonymous" or "de-identified" to communicate the basic concept that data have been stripped of identifying personal information.

- **Consent.** Consent to data processing can be described in many ways, but it is important to capture whether individuals have given active consent (aka affirmative, express, or opt-in consent) or passive consent (aka implicit or opt-out consent).
  - Other descriptors may carry their own connotations, which IDS should be careful about invoking.
    - *Informed consent* often appears in medical or research settings and suggests a very high level of consent, often involving detailed, one-on-one evaluations with researchers.
    - V*oluntary or freely given* consent may recall workplace data agreements, such as for biometric screening for workplace wellness programs, which may sometimes come with incentives for sharing personal data.

- **Data is/data are.** Data are only plural when you are speaking to sophisticated data users or researchers. When speaking with general audiences, use the singular.

- **Data subject.** There is a person behind every administrative record, and IDS should demonstrate empathy in describing data about people and communities.
  - Are you *tracking* or *capturing* or *collecting* data points? Try to avoid describing data collection in ways that diminish someone's dignity or autonomy ('capturing' or 'tracking' data about people).
  - Are individuals in your records *data subjects* or *people* or *community members?* Try to avoid characterizing individuals as passive, faceless masses ('data subjects,' 'users,' 'consumers'), which can be distancing and off-putting. Describing groups by their shared characteristics ('students,' 'patients,' or 'clients') can be appropriate, but be careful about inadvertently using contentious or politicized classes (instead of 'citizens,' for example, use 'community members').

- **Data use vs. data sharing.** Consider the words you use to portray the IDS' work carefully.
  - Are you *studying* or *evaluating* administrative data? Are you *using* it, *exploiting* it, or *drawing upon* it? Avoid terms with negative connotations (like 'exploit' or 'manipulate') to describe handling personal data. More technically sophisticated audiences may prefer more precise descriptors ('linking,' 'evaluating'), while lay audiences may prefer more general terms ('using,' 'studying').
  - Be careful when talking about *"data sharing,"* which may raise concerns that personal data is being given to third parties or being made public in an uncontrolled manner. Mention the specific purpose for which data is being shared, any limitations on how the data may be used, and what technical or contractual safeguards are in place that allow the data to be shared without infringing on individual privacy.
- **Necessary vs. nice to have.** When discussing a particular IDS use case, ensure that any data elements you describe as "necessary" are in fact essential to the and are not just "nice to have." Claims that data elements are "necessary" can act as lightning rods for privacy critics, similar to descriptions of data as "anonymous." While lay audiences are unlikely to split hairs on such matters, being drawn into factual or methodological debates with outside experts about the data points needed for an analysis can derail your broader communication strategy, particularly when sensitive personal data is at issue.