NOTHING TO HIDE:

Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems

OCTOBER 2018

FUTURE OF PRIVACY FORUM

ACTIONABLE INTELLIGENCE FOR SOCIAL POLICY

Acknowledgements: We extend our thanks to the AISP Network and Learning Community, whose members provided their support and input throughout the development of this toolkit. Special thanks to Whitney Leboeuf, Sue Gallagher, and Tiffany Davenport for sharing their experiences and insights about IDS privacy and engagement, and to FPF Policy Analyst Amy Oliver and FPF Policy Intern Robert Martin for their contributions to this report.

We would also like to thank our partners at Third Sector Capital Partners and the Annie E. Casey Foundation for their support.

This material is based upon work supported by the Corporation for National and Community Service (CNCS). Opinions or points of view expressed in this document are those of the authors and do not necessarily reflect the official position of, or a position that is endorsed by, CNCS or the Social Innovation Fund.

TABLE OF CONTENTS

Introduction ... 2
- Why engage and communicate about privacy? ... 2
- Using this toolkit to establish social license to integrate data ... 2

Communicating about Integrated Data ... 4
- Sharing a clear and confident public message about integrated data and privacy ... 4
- Step 1) Set your communication goals ... 4
- Step 2) Develop your communications strategy ... 4
- Step 3) Develop specific messages that speak to your audience ... 5
- Step 4) Identify your communications channels and tools ... 6
- Step 5) Mobilize your allies ... 7

Engaging Stakeholders around Integrated Data ... 8
- Building strong and sustainable relationships with those who care about data and privacy ... 8
- Step 1) Establish your engagement strategy and resources ... 8
- Step 2) Identify and map your stakeholders ... 9
- Step 3) Prepare for your engagement activities ... 9
- Step 4) Convene and engage your stakeholders ... 10
- Step 5) Follow through and follow up ... 10

Conclusion ... 11

Appendix A – Understanding Data Privacy ... 12
- A.1: Privacy basics ... 12
- A.2: Integrated data privacy ... 13
- A.3: Privacy Fair Information Practice Principles (FIPPs) ... 14
- A.4: Privacy tools and resources ... 15

Appendix B – Communications Talking Points and Exercises ... 17
- B.1: Talking Points – Describing and distinguishing your IDS ... 17
- B.2: Talking Points – Setting reasonable privacy expectations ... 18
- B.3: Talking Points – Responding to others' privacy expectations ... 19
- B.4: Talking Points – Tips on language and privacy lingo ... 21
- B5: Exercise – Elevator Pitch ... 23
- B6: Exercise – Advanced Elevator Pitch ... 24
- B7: Exercise – Data Benefit Analysis ... 25

Appendix C – Engagement Worksheets, Checklists and Sample Materials ... 26
- C.1: Worksheet – Strategic Engagement Planning ... 26
  - 1. What are our objectives for this engagement? ... 26
  - 2. What is the environment for this engagement? ... 26
  - 3. What are our resources for engagement? ... 27
- C.2: Worksheet – Stakeholder Mapping ... 29
  - 1. Identify your potential stakeholders ... 29
  - 2. Assess your potential stakeholders' interests ... 30
  - 3. Prioritize your key stakeholders ... 30
- C.3: Worksheet – Pre-Engagement Planning ... 31
  - 1. Prepare answers to basic questions on process and substance ... 31
  - 2. Identify what informational or discussion materials you will need ... 32
- C.4: Worksheet – Convening Stakeholders ... 33
  - 1. Deciding when to engage ... 33
  - 2. Deciding what engagement activities are the best fit for your IDS and use case ... 34
  - 3. Engaging Inclusively ... 34
  - 4. Engagement Matrix ... 35
- C.5: Worksheet – Closing the Engagement ... 37
- C.6: Checklist – Meeting Facilitation ... 38
- C.7: Checklist – Public Engagement Meeting Planner ... 39
- C.8: Sample – Stakeholder Meeting Agenda, Privacy Specific ... 42
- C.9: Sample – Interagency IDS Retreat Agenda ... 44
- C.10: Sample – IDS Stakeholder Analysis ... 45

Appendix D – Additional Resources ... 46

Endnotes ... 48

INTRODUCTION

Data-driven and evidence-based social policy innovation can help governments serve communities better, smarter, and faster. Integrated Data Systems (IDS) use data that government agencies routinely collect in the normal course of delivering public services to shape local policy and practice. They can use data to evaluate the effectiveness of new initiatives or bridge gaps between public services and community providers.

Respecting privacy is paramount to IDS' success. The use of IDS to link sensitive personal data is typically governed by stringent local, state, and federal privacy laws and regulations, as well as rigorous technical safeguards and ethical norms. Nevertheless, individuals and communities routinely have questions and concerns about how their information is used and protected.

For lasting success, IDS need to develop **"social license"** to integrate data. Ultimately, societal acceptance and approval depend not merely on legal compliance with privacy rules, but on each IDS' legitimacy, credibility, and public trust.[1] Inclusive public engagement and effective communications around privacy are necessary for IDS to build trust in the public sector and to create strong, sustainable relationships with the communities they serve.

We hope these resources will help IDS and government leaders engage stakeholders in establishing appropriate safeguards for integrated data and increase communities' trust in the value of IDS.

Why engage and communicate about privacy?

- Proactive engagement is the best way to create an environment in which people trust your proposed or established IDS.
- Integrating your stakeholders' skills and expertise (as well as their data) can improve your IDS design and implementation.[2]
- Effective public communication can create legitimacy and public trust in your IDS, proactively address concerns raised by internal and external stakeholders, and lay a foundation to develop your social license to use administrative data.
- IDS have both legal and ethical obligations to be transparent and accountable in the use of administrative data to benefit communities.
- Failing to address stakeholders' privacy perceptions and concerns—even with strong privacy safeguards in place—can disrupt or conclude your IDS.[3]
- Building sustainable relationships within your communities creates an opportunity to talk about data benefits and privacy solutions, not just privacy problems.

Using this toolkit to establish social license to integrate data

The path to social license for integrated data lies in IDS establishing sound, two-way communications; empowering stakeholders; and continually serving the public good.[4]

Above all, IDS seeking to establish their social license to integrate data must remember to:

- **Build trust through communication and engagement.** IDS must seek public buy-in by communicating and demonstrating the value of integrated data for social policy improvement and innovation. It is not enough to comply with legal requirements for linking personal data. As public servants handling sensitive and personally identifiable data, IDS and government leaders should strive to earn the trust, credibility, and legitimacy necessary for a lasting social license to operate. This means inviting a diverse set of stakeholders to be a part of the decision-making process about how integrated data is used and protected within their communities and ensuring that IDS activities respect stakeholders' rights and serve their goals.
- **Be flexible and invest in relationships.** Because each group of IDS stakeholders and IDS use case has unique goals, capabilities, and cultural context, the tools described in this toolkit can and should be flexibly implemented. Users should adapt and employ the combination of activities from each section that best fits their needs based on the scale, scope, and context of their data-driven activities. In the long term, government and IDS leaders must also invest the appropriate resources and staff to

maintain sustainable relationships and ensure that stakeholder engagement and communications efforts are implemented meaningfully.

- **Follow through with good data policies and practices.** Effective engagement and communication about privacy issues must be grounded in strong data policies and practices that ensure personal data is used legally, ethically, and safely.[5] If a data-driven activity is not legal, ethical, or safe for the community, no amount of stakeholder engagement or communication can overcome these fundamental flaws. And if government or IDS leadership cannot follow through on their privacy safeguard promises, no lasting public trust or social license can be built. IDS need to: visibly incorporate stakeholder input into their data practices; effectively safeguard personal data; and proactively share the benefits of their work so that their communities can trust and value it.

This toolkit provides IDS stakeholders with the necessary tools to support and lead privacy-sensitive, inclusive stakeholder engagement efforts. A narrative step by step guide to IDS communication and engagement is supplemented with action-oriented appendices, including **worksheets, checklists, exercises,** and **additional resources.**

COMMUNICATING ABOUT INTEGRATED DATA

Sharing a clear and confident public message about integrated data and privacy

Integrated data can be a valuable tool for evaluating and implementing policy and programs that address a wide range of community needs—but only if policymakers, community members, and other stakeholders know about and trust in the IDS. In communities without a **clear understanding** of how personal data is integrated, safeguarded, and used for the public good, there can be no social license for IDS.

IDS must actively **listen to** and **address** their communities' privacy and equity concerns, whether real or perceived. Ignoring or waiting to tackle those perceptions until later won't make them go away; instead the lack of responsiveness will sow mistrust, undercut otherwise valuable work, and slow the adoption of integrated data nationwide.

A proactive, people-focused communications strategy lays the foundation for both educating and engaging IDS stakeholders in privacy decision-making. In this section, we introduce key communications strategies and messages about integrated data and privacy. We encourage you to develop a communications approach that is:

- ✓ **Clear** – Be honest, direct, and transparent about privacy and personal data
- ✓ **Confident** – Show the value of integrated data and share your successes
- ✓ **Reciprocal** – Listen to your community and create spaces for others' voices

Step 1) Set your communication goals

Hopefully, proactive outreach to your stakeholders will someday become a routine affair. Until it does, however, your IDS should be thoughtful and intentional about what you are trying to achieve each time you communicate with your stakeholders about privacy protections and responsible data use. This will help keep your messages clear and consistent.

Some key goals for IDS privacy communications might include:

- Earning the trust of the community you are serving.
- Educating the public about administrative data, program evaluation, and social policy innovation.
- Sharing meaningful stories to show how integrated data has impacted people and communities.
- Assuaging concerns about how you are using and protecting personal data.
- Getting decision-makers to approve new data-driven approaches.
- Promoting evidence-based policymaking at a local, state, or national level.
- Creating a common understanding of integrated data in your community to lay a foundation for robust public engagement around privacy and data use.
- Encouraging stakeholders to participate in upcoming engagement activities.

Your communication objectives will likely vary depending on your audience, as will your strategy for achieving them.

Step 2) Develop your communications strategy

Once your IDS is on the same page about the goals you are trying to achieve, the question becomes *how*?

A confident, positive communications posture is important for successful long-term relationships with stakeholders. IDS should strive to:

- **Be proactive.** Focus on *showing* specific examples of the benefits of integrated data for improving services and policy initiatives rather than just telling people about them. Demonstrate that privacy rights are important and that your IDS is committed to handling data responsibly. Make sure you are getting ahead of misinformation or confusion. Reach out and establish open lines of communication with stakeholders before there is a problem.

- **Know your audience.** Emphasize how integrated data help *people*, not processes. While some stakeholders may appreciate numbers, most gravitate more to narratives about outcomes and impact. Technical or expert audiences may want to know more about specific privacy safeguards. Lay audiences or community members may be interested in more philosophical responses about values and goals.
- **Learn from others.** Pay attention to campaigns supporting evidence-based policymaking at the local, state, and federal level. Observing these efforts can help you identify potential collaborators, successful (or unsuccessful) communications strategies, and effective privacy safeguards.
- **Articulate a clear and public purpose for integrated data.** Use language that is simple and direct enough for both community members and policymakers to understand. Provide examples of how and why administrative data are being integrated.
- **Acknowledge and address community concerns.** Data integration involves inherent risks and benefits. Rather than minimizing stakeholders' concerns, describe the safeguards in place to diminish privacy impacts to individuals and communities, and any approaches available to mitigate harm.
- **Highlight how you will be accountable for responsible data use.** Educate stakeholders about existing laws and policies that govern responsible data use. Clearly communicate your metrics and goals to the communities you serve and enable them to hold you accountable. Celebrate small successes and milestones along the way, to create and sustain momentum.
- **Keep privacy conversations about privacy.** When discussing data-driven policy initiatives, privacy concerns can easily be conflated with or co-opted by other political, social, or technological debates. Be prepared to respond to these kinds of derailments by steering the conversation back to data privacy, and addressing related concerns directly at the next opportunity.

Operationally, your IDS can support these strategies by:

- **Being flexible.** As new opportunities and challenges arise, your IDS will need to be able to respond quickly. Be ready to pivot as communications resources change, new stakeholders or counter-campaigns emerge, or some materials prove more effective than others. Ultimately, your goal should be to communicate in whatever ways are best for your stakeholders, even if it means learning new skills or developing new materials.
- **Documenting your communications goals and strategy.** Creating a written resource that clearly defines and tracks your communications activities can be an important tool. Being able to share who has been contacted about what, which materials are in development, and what resources are already available, for example, helps ensure everyone is on the same page throughout the IDS lifecycle. This type of document can also be shared with your allies and partners.
- **Investing in communications.** Effective communications materials don't just spontaneously appear, as this work requires time, skill, and effort. Depending on your IDS' partnerships and networks, it may be possible to reduce costs by accessing free or pro bono work by experts or by leveraging existing materials from peer networks.

For help preparing your IDS to discuss privacy and equity impacts, see the Elevator Pitch, Advanced Elevator Pitch, and Data Benefit Analysis exercise below in Appendices B.5-B.7.

Step 3) Develop specific messages that speak to your audience

With high-level goals and strategies in mind, your IDS should begin crafting specific messages and materials that will resonate with your stakeholders. This will be an iterative process, and as you learn more about your stakeholders you will likely revise and refine your messages. You may also need to create different versions of the same materials and tailor them to your different audiences, particularly as you work to reach marginalized or traditionally underrepresented groups.

As a baseline, each member of the IDS should be able to clearly and specifically articulate the IDS' mission and commitments to safeguarding individual privacy. Other key messages for IDS privacy communications include:

- **What an IDS is and what makes it special.** Your IDS is likely one of many efforts utilizing the community's administrative data. It is important to be able to describe what makes the IDS unique and valuable to the community, both to avoid confusion among your stakeholders and to prevent the IDS' activities and reputation from being conflated with public perceptions of other efforts or organizations.
- **What you are doing to protect privacy.** An important but difficult part of communicating about privacy is proactively educating stakeholders about reasonable expectations for privacy safeguards and

reasonable limitations on data collection and use. Some may not appreciate what can—or cannot—realistically be done with integrated data, and so may overestimate the risks to individual privacy and civil liberties. It is therefore important to be able to concisely describe what integrated data will and will not be used for, and how decisions about those uses will be made.

- **What stakeholders can do to get involved.** For many people, personal privacy is deeply emotional and its real or perceived absence may leave them feeling vulnerable, exposed, or out of control. This is why trust and transparency are essential to building successful and sustainable IDS, and why IDS must try to fully understand and appreciate their communities' perspectives about how and when to use data appropriately. There may be a variety of reasons that community members support or object to a particular data-driven use case. Make clear that you are committed to listen, no matter what stakeholders have to say. When stakeholders feel out of control of their own data, give control back to them by creating opportunities for meaningful input and influence on the IDS.

For samples and tips for crafting your own messages, see the Communications Talking Points, Tips on Language and Privacy Lingo, and Elevator Pitch exercises in Appendices B.1-B.5.

Step 4) Identify your communications channels and tools

Depending on your stakeholders and your messages, some communication channels may be better suited for your IDS' efforts than others.

Factors to consider when choosing which channel include:

- **Active vs. passive participation.** While some communications platforms are largely passive or static (websites, newspapers, reports, etc.), others may offer more active or dynamic engagement opportunities (social media, interactive dashboards, Q&As, etc.). Passive tools are particularly helpful for sharing general informational and educational materials, while two-way communication tools may be better for addressing more nuanced or fact-specific questions about integrated data privacy. Person-to-person communications or videos may also help foster a sense of familiarity and ease that documents alone cannot achieve.

POTENTIAL COMMUNICATION ACTIVITIES

POTENTIAL COMMUNICATIONS CHANNELS COULD INCLUDE:

- **Broadcast media**, such as TV or radio.
- **Community-based** media, such as community newspapers, blogs, or events.
- **Digital media,** such as social media, email, or websites.
- **Face-to-face.**
- **Folk media,** such as storytelling or cultural performances.
- **Print media,** such as newspapers or magazines.
- **Specialized media,** such as multilingual TV stations or print media in Braille.

POTENTIAL COMMUNICATIONS TOOLS COULD INCLUDE:

- **Commenting opportunities,** such as formal notice and comment mechanisms, annotation sites, or crowdsourcing platforms.
- **Informative opportunities,** such as mailings, press releases, infographics, fact sheets, case studies, white papers, informational bulletins, academic publications.
- **Interactive opportunities**, such as dashboards, dynamic infographics or visualizations.
- **Interpersonal opportunities,** such as Q&As, interviews, social media, classes/trainings, or in-person meetings.
- **Promotional opportunities,** such as op-eds, PSAs, posters, or advertisements.

- **Data tools.** Giving stakeholders free access to aggregate data or data visualizations can be a powerful way to engage and empower communities. At the same time, data divorced from its context may be confusing or hard to interpret. If you invest in public-facing data tools, be sure to demonstrate how users can use them to tell stories (such as with videos, FAQs, and introductory guides) and pair data tools with analytic guidance and clear metadata.
- **Depth.** The medium is the message: if your point about integrated data privacy belongs in an academic paper, don't try to force it into a tweet. Be thoughtful about how much depth and detail is appropriate for each channel you employ, acknowledging that there will be tradeoffs between length, nuance, and accessibility.

- **Inclusivity.** While mass media channels may have the broadest numeric reach, specialized media may be more effective for reaching marginalized or traditionally underrepresented groups. Similarly, digital media may be quick and cheap, but may not be effective at reaching less technologically-connected communities (older communities, persons with certain disabilities, or communities disconnected by the digital divide). Consider using public facilities like libraries, community centers, and neighborhood service providers as accessible, local information repositories.

It is important to be creative and flexible in picking your communications tools—it is your job as the communicator to meet your stakeholders wherever they are, even if it means adapting to a new platform yourself.

Step 5) Mobilize your allies

Finally, you should enlist your allies to help validate your messages and amplify your communications. By partnering with others, you may be able to reach more diverse communities, access new resources, and empower your stakeholders.

When communicating about privacy and integrated data, IDS should strive to:

- **Empower others to be your messenger.** Enlist trusted community members or organizations to validate your IDS' positive impacts and your commitment to privacy. Have supporters and allies within your stakeholder communities help you develop accurate and accessible materials, identify additional communications channels, and amplify your messages within their networks. Provide your messengers with the tools and knowledge to advocate on your behalf, including clear answers about how personal data will be used and protected, and what benefits and risks may arise from a particular use case.
- **Be proactive advocates for ethical data use and privacy-preserving data sharing.** Be an active participant when relevant policymakers or peer organizations have policy discussions about administrative data, appropriate data use, and privacy. Support privacy standards and best practices across your communities, and share best practices and lessons learned with your peers.
- **Foster community engagement.** Publicize engagement opportunities around data, privacy, and decision-making. Include policymakers and people from the communities you serve in important conversations about integrated data and privacy. Listening to your stakeholders is the only way you will learn what they need and how data can help.

ENGAGING STAKEHOLDERS AROUND INTEGRATED DATA

Building strong and sustainable relationships with those who care about data and privacy

To achieve lasting success and establish social license for data-driven policy innovation, IDS and partners must do more than simply talk about privacy—they must create ways for their stakeholders to **meaningfully engage** with them around data and privacy issues. When individual rights and community interests in data are at stake, collaboration with community members, civil society, political and agency champions, and other stakeholders is not only good policy, it is essential to informed and ethical decision-making.

For privacy engagements to be meaningful, stakeholders must be able to have true influence over the design and direction of the IDS and its use cases. Hollow or token involvement in the process defeats the purpose of engagement and undercuts trust in the IDS as a whole.

The International Association for Public Participation has developed a "Participation Spectrum" to help organizations evaluate how actively engaged participants will be. IDS should strive to **"empower," "collaborate,"** or **"involve"** stakeholders wherever possible.[6] Rather than simply relying on stakeholders to react to ideas and proposals, IDS should also consider how to incorporate stakeholders' skills and expertise directly.[7]

LEVELS OF PUBLIC PARTICIPATION GOALS	
Inform	To provide the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions.
Consult	To obtain public feedback for decision-makers on analysis, alternatives and/or decisions.
Involve	To work directly with the public throughout the process to ensure that public concerns and aspirations are consistently understood and conisdered in decision making processes.
Collaborate	To partner with the public in each aspect of the decision including the development of alternatives and the identification of the preferred solution.
Empower	To place final decision-making in the hands of the public.

In this section, we provide a 5-step roadmap for stakeholder engagement about integrated data and privacy.[8]

We encourage you to adapt this guide to fit *your* IDS' needs, resources, and vision as you build stakeholder engagement processes that are:

- ✓ **Strategic** – Support active participation in ways that lead to visible results
- ✓ **Inclusive –** Seek out diverse voices and create spaces that are welcoming to all
- ✓ **Sustainable –** Build lasting relationships with your community

Step 1) Establish your engagement strategy and resources

Before actively involving external stakeholders around the IDS or a particular use case, IDS must first agree internally upon the scope and objectives of their engagement. Successful stakeholder engagement activities—particularly around privacy, which requires both technical skills and empathy—require significant investment. However, failing to dedicate the appropriate resources for participatory engagement can mean asking the wrong questions, using the wrong data, not having the right voices at the table, or not being able to deliver on your promises to participants and the public.

As a first step, everyone on the IDS planning team should generally know:

- › What the team wants to achieve by engaging stakeholders;
- › What the environment for engagement is like; and
- › What resources can be committed to the engagement process.

By being honest and specific about these factors up front, the planning team will be better prepared to efficiently leverage stakeholder input. Devoting sufficient time at this stage can ensure ethical use of data and save considerable effort later.

For help thinking through these preliminary scoping questions, see the Strategic Engagement Planning Worksheet below in Appendix C.1.

Step 2) Identify and map your stakeholders

Once the strategic goals of your privacy-related stakeholder engagement process have been set, it is time to identify and prioritize your potential stakeholders. For any IDS engagement, it is important to strike a balance between providing space to hear from an appropriate range of perspectives while still keeping discussions focused and structured enough to be productive. By taking time early on to identify your potential stakeholders, consider their interests and positions, and formally map out the most interested and influential players, you will be able to make more informed choices later when planning specific engagement activities.

At this stage, IDS planning teams should:

- Brainstorm potential stakeholders for your IDS or this specific use case, thinking broadly and inclusively about who may impact or be impacted by your use of administrative data (including possible supporters and possible opponents);
- Assess those potential stakeholders' interests, such as where they stand on integrated data and privacy issues and how they can help or hinder your use case; and
- Prioritize key stakeholders by mapping potential participants by their likely interest and influence in your IDS or use case's success.

IDS planning teams should focus on including stakeholders with diverse backgrounds and expertise, given the variety of perspectives that communities and individuals may hold about privacy and appropriate uses of personal data. Even if some stakeholders do not end up participating in this specific engagement process, working to understand them and their interests is imperative for establishing strong and sustainable relationships for the future.

For help thinking through these brainstorming, assessment, and mapping activities, see the Stakeholder Mapping Worksheet below in Appendix C.2 and the Sample IDS Stakeholder Analysis in Appendix C.10.

Step 3) Prepare for your engagement activities

Many of your stakeholders may be unfamiliar with the IDS model, mission, and potential use cases. It may be necessary to educate your stakeholders before engaging them. Baseline informational materials about the IDS, its proposed use cases, and approach to privacy are critical tools for ensuring that everyone is on the same page and can meaningfully participate during a particular engagement activity. These baseline informational materials should be customized to support the strategic goals and key stakeholders identified in the previous steps. This involves:

- Preparing your IDS to answer basic questions about the engagement process, your IDS/use case, and your IDS' proposed approach to data and privacy issues; and
- Creating any necessary informational or discussion materials.

You should not arrive at an engagement activity with fixed plans about how data will be used and protected (which limits your stakeholders' opportunities for meaningful input), but neither should you arrive with a completely blank slate (which can waste everyone's time and energy). Strive to create clear and detailed proposals for how the IDS or use case *might* progress for stakeholders to respond to, and, where there is room for flexibility, encourage stakeholders to suggest their own alternatives.

For example:

- *Too fixed:* Asking for a rubber stamp approval of a fully drafted governance structure.
- *Too open-ended:* Asking how stakeholders want their data to be used.
- *Meaningful and productive:* Asking stakeholders if they are comfortable with specific use cases, or to prioritize a list of potential research projects.

For help thinking through these preliminary questions, see the Pre-Engagement Planning Worksheet below in Appendix C.3.

Step 4) Convene and engage your stakeholders

For any IDS initiative or use case, there will likely be multiple phases and types of engagement. You must strike a balance between providing enough structure for your engagement activities to be productive while also building in enough flexibility to adapt to group dynamics or sudden inspiration.

While not all stakeholders need to be included in each phase or activity, you should think imaginatively about what environments will be most conducive to (1) meaningful outcomes for your IDS and (2) meaningful participation for your stakeholders.

At this stage, IDS planning teams should:

- Decide *when* and *how* in your IDS lifecycle to include engagement and involvement activities;
- Take care of logistical details, particularly those that support inclusiveness and diversity (for example, identifying a diverse range of participants for a meeting and scheduling meetings to promote access); and
- Facilitate productive discussions during your engagement activities.

POTENTIAL ENGAGEMENT ACTIVITIES

POTENTIAL IN-PERSON ENGAGEMENT ACTIVITIES COULD INCLUDE:

- **One-on-one meetings,** such as interviews or surveys.
- **Small group meetings,** such as community advisory committees, charrettes, focus groups, roundtables, expert panels, or working groups.
- **Large or public meetings,** such as town hall meetings, public hearings, open houses, hackathons, public workshops, public debates, or community summits.

POTENTIAL REMOTE ENGAGEMENT ACTIVITIES COULD INCLUDE:

- **Interactive opportunities,** such as public voting or ballot initiatives, surveys, questionnaires, online forums or listservs, or social media discussions.
- **Active opportunities,** such as formal notice and comment mechanisms, annotation sites, or crowdsourcing platforms.
- **Passive opportunities,** such as press releases, fact sheets, white papers or informational bulletins.

Under-represented groups provide valuable experiential expertise, cultural assets, and knowledge to IDS that may otherwise be overlooked.

You can learn what is the right fit for your set of stakeholders through experience or by asking others who have hosted engagement activities within your community. Stakeholder engagement activities should not be viewed as one-off events, but rather as steps to building sustainable relationships within your community.

Importantly, IDS planning teams must also be attentive to structural or cultural barriers that may have traditionally kept some individuals or groups from participating in public engagements. Providing **inclusive** spaces and platforms is critical for data-driven and community-focused efforts like IDS, which should recognize diversity as both a strength and an opportunity. Under-represented groups provide valuable experiential expertise, cultural assets, and knowledge to IDS that may otherwise be overlooked.

IDS engagement planning teams should also **actively** facilitate stakeholder discussions, whether in-person or virtual. This includes framing the discussion and working with stakeholders to identify guiding principles; set an appropriate agenda; smooth logistical glitches; create verbal and physical spaces for all participants to contribute, especially those newer or less confident in their roles; keep discussions on topic; manage misunderstandings; and defuse tension and/or help stakeholders reach consensus.

For help implementing your engagement activities, see the Convening Stakeholders Worksheet (Appendix C.4), the Meeting Facilitation and Public Engagement Meeting Planner (Appendices C.5 and C.6), and the Sample Stakeholder Meeting Agenda and Sample Interagency IDS Retreat Agenda (Appendices C.8 and C.9) below.

Step 5) Follow through and follow up

Finally, now that you have heard from your stakeholders directly, you must decide how you will respond to their input. Particularly when addressing issues like privacy and responsible data use, it is important to recognize that successful stakeholder engagements involve flexibility, compromise, and iterative project development. Once the IDS's next direction is decided, planning teams will need to develop detailed action plans and communicate with stakeholders about the outputs of the engagement.

The whole IDS' credibility depends on transparency at this final step in the engagement process,[9] and IDS planning teams should not consider a stakeholder engagement process concluded until:

- Final decisions have been made to accept or take action on *some, all, or none* of the stakeholder group's recommendations; and
- Those decisions have been communicated back to your stakeholders, along with the reasons why and a plan to put those choices into action.

A detailed report documenting the engagement process, including its initial goals and assumptions, key discussion points, lessons learned, and how stakeholder input was incorporated can facilitate future engagements and demonstrate the value to internal and external stakeholders. This is an opportunity for IDS to thank stakeholders for their participation, to invite further feedback, and to identify opportunities for future IDS use cases and engagement activities.

For help thinking through these final steps, see the Closing the Engagement Worksheet below in Appendix C.5.

CONCLUSION

IDS not only improve public policy decisions, they create important opportunities for communities to engage and communicate about privacy and responsible data use. In order to secure social license to integrate and use personal data for policy innovation, IDS must **earn trust, build lasting relationships,** and **establish good data policies and practices.**

IDS must learn how to share a clear and confident public message about integrated data and privacy. They must also learn to build strong and sustainable relationships with those who care about data and privacy, and to create inclusive, productive, and meaningful spaces for those stakeholders to engage. The path to social license for integrated data lies in IDS establishing sound, two-way communications; empowering stakeholders; and continually serving the public good.

We hope that these stakeholder communications and engagement guides, as well as **worksheets, checklists**, **exercises,** and **additional resources** available in the attached Appendices, will help IDS as they develop their own messages and materials around privacy and responsible data use.

APPENDIX A: UNDERSTANDING DATA PRIVACY

In order to most effectively engage and communicate with stakeholders about privacy, IDS should be familiar with the basics of modern privacy and data protection. Understanding common privacy principles, risks, and resources will help focus your efforts to gather community input and create appropriate privacy safeguards.

A.1: Privacy basics

Data privacy is...

- **A fundamental right.**[10] Individual privacy rights are recognized in the U.S. Constitution, the Declaration of Human Rights, and in over 80 countries around the world. Privacy rights also provide the foundation for other important rights, including self-determination and free expression.
- **Dynamic.** Some of the most common aspects of data privacy include:
  - Control over personal information flows;
  - Freedom of thought and exploration; and
  - Protection of one's dignity and reputation.
- **Subjective.** Each person has unique privacy preferences and expectations—what feels invasive or creepy to one person may be innovative or cool to another. These preferences and expectations are influenced by many factors, including a person's familiarity with data systems, experiences of marginalization, cultural background, and trust in data-holding organizations.[11]
- **Contextual.** Whether it is appropriate to use or share personal data in a particular manner depends on ever-evolving social and ethical norms, as well as legal frameworks. In order to understand your community's norms about integrating data, it is essential to communicate and engage directly with members of your community.
- **Power.** The more information that one person or organization has about another, typically, the more that party may influence or exert power over the other. Privacy protections help individuals and communities maintain their autonomy and freedom when their information is used by governments and other organizations.

Data privacy is *not*...

- **Secrecy.** Seeking to protect privacy does not mean preventing all others from learning information about you. On the contrary, privacy is about creating conditions in which individuals will trust others enough to share their personal information.
- **Security.** Although data privacy and data security are closely related, a perfectly secure data system may still violate individual privacy if authorized users acting within an organization or system's normal capabilities use personal data in unexpected or inappropriate ways.[12]

Although privacy definitions may seem abstract and subjective, privacy risks can be significant and concrete. Failing to adequately safeguard data or using it inappropriately can have serious and lasting consequences for individuals.

Common privacy risks for individuals include:[13]

- **Financial** risks, such as identity theft or fraud;
- **Physical risks,** such as stalking or burglary;
- **Reputational risks,** such as embarrassing rumors or damaging photos; and
- **Dignitary risks,** such as a loss of autonomy or opportunity when a person is profiled or discriminated against by an automated decision-making system.

Nevertheless, privacy risks may not always be immediately apparent. Many times, privacy risks for individuals are...

- **Incremental.** As datasets grow and are combined over time, so does the likelihood of a data breach, a successful re-identification attack (singling out individuals in seemingly non-personal data), or a discriminatory impact on vulnerable, historically marginalized, and/or over-surveilled communities.
- **Unequal.** Privacy risks may also accrue unevenly throughout society. If not addressed in advance, some community members may reap the benefits of data-driven governance, while others bear all of the privacy risk burden.
- **Non-obvious.** Certain privacy risks are more impactful or more likely to occur for particular groups, and can be overlooked by program

designers who have not specifically incorporated those individuals' inputs. For example, publishing the contact information of everyone who attended a meeting will have different implications for an elected official than a domestic violence survivor.

- **Intrusive.** Privacy is closely tied to feelings about self-control and autonomy, and its real—or perceived—loss can leave people feeling vulnerable, exposed, and out of control of their own lives. In these situations, individual and community behavior can be chilled, relationships harmed, and trust lost.

Because privacy risks can be so varied, it is critical to engage diverse stakeholders in discussions and decision-making about integrating personal data. Incorporating non-traditional voices within your stakeholder groups will strengthen your ability to foresee and address privacy or equity externalities arising from the IDS' work.

A.2: Integrated data privacy

Privacy risks are not hypothetical, and neither are public responses to them. Failure to protect individuals' privacy—including miscommunications or silence by organizations about how personal data will be used and protected—can lead to lasting public mistrust,[14] internal protests,[15] project collapse,[16] and even legislative backlash.[17]

Common risks for organizations (including IDS) that fail to handle privacy correctly, or are *perceived* to fail at privacy, include:

- **Financial** risks, such as lawsuits or statutory damages, or the withdrawal of funding;
- **Reputational** risks, such as loss of public trust and support in the IDS; and
- **Regulatory,** such as new legislative restrictions on administrative data use and sharing.

IDS must be mindful that, as representatives of state and local government, your use of individuals' personal data can be particularly fraught. IDS face several unique hurdles to earning public trust and social license to use their community's personal data, including:

- **History.** Over the course of history, both governments and researchers have mistreated and misused personal data.[18] IDS should be aware that those scars have lingered, and appreciate that some individuals and communities have valid reasons to be reluctant about data sharing.
- **Big Brother looms large.** When data is collected and used by government institutions, privacy risks—and fears—can become amplified. To many communities, frequent data collection by government agencies, even for beneficial purposes, can feel indistinguishable from Big Brother-type surveillance. Historically marginalized populations, such as people of color and those living in poverty, in particular may be the target of multiple, concurrent data collection efforts by local, state, and federal agencies.
- **Consent.** Most privacy laws require organizations to get an individuals' consent before using their personal information, particularly when the data is sensitive. The nature of most IDS activities, however, means that they are secondary uses of administrative data and such consent isn't feasible. While IDS activities *are* specifically permitted under those same laws, many people may be unfamiliar with those exceptions or may simply expect an opportunity to consent by default.
- **Data-driven inequalities.** There is a growing public, private, and academic conversation about how data-driven tools may reflect or reinforce discrimination and bias, even inadvertently.[19] The use of administrative data by algorithmic systems, whether by IDS or other organizations, raise serious ethical questions and may color public perceptions of *other* data uses.
- **Trust.** The perception that personal data will be used in unexpected ways or will not be kept private and secure can undermine individuals' and communities' trust in government. At its extreme, individuals who are afraid of how data about them could be used may even provide false information or forgo government services.[20]

Meaningful stakeholder engagement and communication, as well as strong privacy protections, can help put power back in the hands of individuals and communities. Protecting privacy is critical to respecting individuals' rights and maintaining individuals' trust in government.

Some uses of personal data will carry more inherent privacy risks than others. For IDS, these include...

LOWER RISK	HIGHER RISK
Non-sensitive data (e.g., demographic or contact information)	Sensitive data (e.g., health, financial, criminal justice, location, or education data)[21]
Aggregated data	Individual records
Data about groups	Data about individuals
Cross-sectional research	Longitudinal research
Evaluating outcomes	Predicting outcomes
Policy analysis and research	Case management, enforcement, adjudication

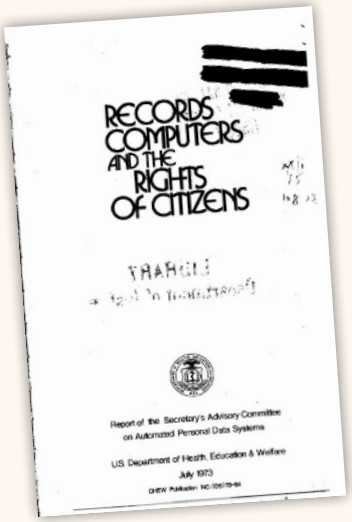
Make sure your IDS is prepared to differentiate between these distinct types of data and distinct data uses in conversations about privacy risks and potential benefits.

The goals of IDS serve important social, economic, and democratic functions; however, if citizens do not trust that their data will be protected or do not see the benefits of IDS use for research and evaluation, they could begin to fear administrative data and government services as tools of surveillance, rather than tools for change.

A.3: Privacy Fair Information Practice Principles (FIPPs)

In order to effectively address privacy risks, privacy professionals and policymakers look to the Fair Information Practice Principles (FIPPs). The FIPPs serve as the common language of privacy and are the basis of all privacy laws around the world. Originating in the 1970s and 80s, the FIPPs consist of eight core principles[22]:

- **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.
- **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.
- **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 fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.



- **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except with the consent of the data subject or by the authority of law.
- **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.
- **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.
- **Individual Participation Principle:** An individual should have the right:
  - to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating 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;
  - to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
  - to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

For many IDS, there may be specific laws or policies that dictate how personal data should be handled and protected for certain activities. But there may also be times that the laws and policies do not clearly capture IDS activities, or where an IDS wants to go above and beyond basic compliance. In these situations, IDS can look to the FIPPs for guidance.

In general, IDS activities lend themselves more strongly to some FIPPs than others. The consent and use/purpose limitation principles in particular seem to conflict with the goals of IDS. However, other FIPPs directly support a commitment to privacy-protective integrated data activities, including the principles of accountability, openness, security, and, in some circumstances, individual participation.

Importantly, IDS should remember that the FIPPs are *principles* for privacy protections, not absolute laws. They can and should be adopted flexibly, to maximize the benefits of integrated data while minimizing the risks to individual privacy. For example, while IDS may find that gathering individual consent is infeasible, they may place a stronger emphasis on other FIPPs, such accountability and openness, through robust stakeholder engagement processes.

A.4: Privacy tools and resources

Ultimately, effective engagement and communication on privacy issues must be grounded in strong data policies and practices. While this section is not intended to provide the components of a comprehensive IDS privacy program, it will help IDS stakeholders and their communities explore key privacy tools and resources. IDS should consult their legal counsel and organizational leadership, as well as appropriate stakeholders, in developing and implementing relevant privacy safeguards.

Some common privacy tools and resources to consider include:

Privacy Control Catalogues describe specific technical and administrative safeguards that can be used to protect and manage data flows.

- National Institute of Standards and Technology (NIST), *SP 800-53 Rev 4: Security and Privacy Controls for Federal Information Systems and Organizations*, *Appendix J: Privacy Control Catalog* (2013), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf.
- Centers for Medicare & Medicaid Services, *Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges, Version 2.0* (2015), https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf.

Privacy Impact Assessments are analyses of how personally identifiable information is collected, used, shared, and maintained by an organization, and is typically used to identify specific privacy risks.

- NIST, *NISTIR 8062: Privacy Risk Management for Federal Information Systems* (2017), http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.
- Bureau of Justice Assistance, U.S. Department of Justice, *Guide to Conducting Privacy Impact Assessments: for State, Local, and Tribal Justice Entities* (2012), https://it.ojp.gov/documents/d/Guide%20to%20Conducting%20Privacy%20Impact%20Assessments_compliant.pdf.
- Information Commissioner's Office (UK), *Data Protection Impact Assessments* (Aug. 2018), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.
- National Commission on Informatics & Liberty (Commisson nationale de l'linformatique et des libertés or CNIL), *Privacy Impact Assessment (PIA): Knowledge Bases* (Feb. 2018), https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf.

Privacy programs ensure that responsibility is established, accountability is maintained, and resources are allocated within an organization to successfully oversee, govern, and use individuals' data.

- Office of Management and Budget (OMB), 81 FR 49689, *OMB Circular No. A-130: Managing Information as a Strategic Resource* (July 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
- Organization for Economic Cooperation and Development (OECD), *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL (July 11, 2013), https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.
- Daniel Solove and Woodrow Hartzog, *The Federal Trade Commission and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913.
- European Commission, *Guidelines on Data Protection Officers ('DPOs')* (Dec. 13, 2016), http://ec.europa.eu/newsroom/document.cfm?doc_id=43823.
- Privacy Technical Assistance Center (PTAC), *Data Governance Checklist* (June 2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Governance%20Checklist_0.pdf.

De-Identification is the process of removing or perturbing identifiable data elements such that individuals can no longer be identified, singled out, or linked to other attributes through their data.

- NIST, *NISTIR 8053: De-Identification of Personal Information 2* (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR .8053.pdf.
- NIST, *SP 800-188 (2nd Draft): De-Identifying Government Datasets* (Dec. 15, 2016), http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft.pdf.
- National Academies of Sciences, Engineering and Medicine, *Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy* (2007), https://www.nap.edu/catalog/24652/innovations-in-federal-statistics-combining-data-sources-while-protecting-privacy.

- National Academies of Sciences, Engineering, and Medicine, *Federal Statistics, Multiple Data Sources, And Privacy Protection: Next Steps* (2017), https://www.nap.edu/catalog/24893/federal-statistics-multiple-data-sources-and-privacy-protection-next-steps.
- Micah Altman et al., *Towards a Modern Approach to Privacy-Aware Government Data Releases*, 30 Berkley Tech. L. J. 1967 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2779266.
- Ira Rubinstein and Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703 (2016), http://lsr.nellco.org/cgi/viewcontent.cgi?article=1534&context=nyu_plltwp.
- Future of Privacy Forum, *A Visual Guide to Practical Data De-Identification*(Apr. 25, 2016), https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification.
- Future of Privacy Forum, *Open Data Privacy Risk Assessment for the City of Seattle*, *Appendix C* (Jan. 30, 2018), https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf.

Data Ethics Frameworks are tools and considerations for helping evaluate whether using data use is unethical and/or whether the benefits and risks are unbalanced.

- Data for Democracy, BrightHive, and Bloomberg, *Community Principles on Ethical Data Practices* (Sept 2017), https://datapractices.org/community-principles-on-ethical-data-sharing.
- Markkula Center for Applied Ethics, *A Framework for Ethical Decision-Making,* Santa Clara University (Aug. 1, 2015), https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/a-framework-for-ethical-decision-making/.
- Department for Digital, Culture, Media & Sport (UK), *Data Ethics Workbook* (June 13, 2018), https://www.gov.uk/government/publications/data-ethics-workbook/data-ethics-workbook.
- Open Data Institute (ODI), *The Data Ethics Canvas* (Aug. 5, 2017), https://theodi.org/article/data-ethics-canvas/.
- Future of Privacy Forum, *Benefit-Risk Analysis for Big Data Projects* (Sept. 2014), https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf.
- Omer Tene and Jules Polonetsky, *Beyond IRBs: Ethical Guidelines for Data Research*, 732 Wash. & Lee L. Rev. Online 458 (2016), https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1044&context=wlulr-online.

APPENDIX B: COMMUNICATIONS TALKING POINTS AND EXERCISES

B.1: Talking Points — Describing and distinguishing your IDS

IDS are not the only groups sharing and analyzing data about their communities. It is important to be able to describe what makes the IDS special and valuable to the community, both to avoid confusion and to prevent the IDS' activities and reputation from being conflated with public perceptions of other organizations. Each member of the IDS should be able to clearly articulate the IDS' mission and commitment to privacy.

Key strategies and messages:

- **Distinguish the IDS from other data-driven organizations.**
  - Our IDS is an interdisciplinary group of public servants dedicated to helping improve our community, not driven by a political or academic agenda or commercial gain.
  - Our IDS is funded by _____. We do not sell or share administrative data for advertising or any other purpose. In fact, that would violate our strict ethical and privacy policies/be illegal.
  - Our IDS sees the value in [other organization's data-driven work], but our focus is on _____.

- **Show the value of integrated data (and the risks of *not* integrating it).**
  - We see data as a public good. Our IDS wants to use integrated data to make our community's public services more effective and efficient for everyone. For example, in other communities IDS have successfully _____.
  - Our IDS' approach focuses on understanding people as individuals (that interact with a range of services) as well as the complex needs of our community as a whole, rather than reducing people or groups to data points.
  - We are working hard to mitigate the privacy risks of integrating data, but we are also considering the risks of *not* integrating data, including _____.
  - Combining information that our public services already collect means we aren't wasting time and money collecting the same data over and over again, and helps us minimize our data footprint.

- **Create confidence in the IDS' commitment and ability to protect privacy.**
  - Privacy is paramount to our work, and we follow strict ethical and legal guidelines to protect it, such as _____.
  - Our agencies have meaningful technical, procedural, organizational, and legal safeguards to protect your privacy, including _____, _____, and _____. (See Appendix A.4 for potential safeguards).
  - Our agencies have collected and protected this information—such as education records, health care data, and criminal justice records—about our community for decades. Our staff are well-trained in safeguarding your privacy, and this experience is now guiding the privacy practices to maintain the same high standards in a digital world.

- **Monitor public perceptions of peer organizations and other data-driven government activities.**
  - Our IDS uses administrative data to evaluate social programs and make them more effective, not to take away anyone's services or benefits.
  - Our IDS includes data that is already collected by public agencies; we do not collect new data at all.

B.2: Talking Points — Setting reasonable privacy expectations

Many stakeholders will not appreciate what is—or is not—realistically possible to do with integrated data, and so may overestimate the risks to individual privacy and civil liberties. Similar confusion often exists about the efficacy and applicability of various privacy safeguards, which can make it difficult for stakeholders to evaluate actual privacy risks and data benefits. It is important to build trust by communicating specifically how data will (and will not) be used and how it will be safeguarded.

Key strategies and messages:

- **Communicate the realistic capabilities and limitations of integrated data.**
  - The analysis of integrated data provides agencies with valuable information about what we are doing well and where we need to make improvements.
  - Although administrative data may include personally identifiable information, the IDS cannot single out or target individuals for action of any kind. We are forbidden by law from doing so and have stringent safeguards and accountability measures in place, such as _____. (See Appendix A.1 for examples).
  - An IDS is only as good as the data it integrates. Before we link data across domains, we work with the agencies that collect it to identify which elements are high quality and relevant to the questions at hand.
  - Even aggregated data (where no personal information is included) about patterns of service use can help our government make decisions about _____ and _____.
  - Integrated data is key to evaluating our current policies, but that is just step one in evidence-based policymaking. Related policy and program changes may still take several months/years to implement.

- **Communicate the realistic capabilities and limitations of your privacy program.**
  - Our IDS has a comprehensive privacy and security policy that clearly outlines the controls and safeguards in place to protect administrative data. (Include any additional, specific safeguards that your IDS is relying on, e.g., only using the data necessary to achieve your goals, never sharing personal data with third parties, access controls, use limits, accountability and audit mechanisms, etc.) (See Appendix A.1 for examples).
  - Privacy and security experts were consulted at every stage of the IDS development process.
  - We comply with multiple federal and state privacy laws that protect administrative data (such as FERPA or HIPAA), and are subject to strict penalties if this data is misused or compromised.
  - Although there are no "silver bullet" solutions to privacy problems, our IDS employs a variety of technical, procedural, legal, and organizational safeguards to significantly reduce privacy risks.
  - We have done our best to anticipate how integrated data will impact our communities, but it is not always possible to eliminate all privacy and security risks. We have several open channels for concerned community members or other stakeholders to raise concerns, complaints, or vulnerabilities, including [link or contact information].
  - Privacy and security management and data protection are on-going systems that are continuously monitored, updated, and supported by trained personnel to ensure they meet the highest standard over time, not just at initial implementation.

- **Articulate the benefits and risks of innovative data use.**
  - Our IDS seeks to maximize data's benefits to the community, such as using data to ensure tax dollars are used efficiently and that our public services are being distributed equitably and effectively within our community—while minimizing risks.
  - We have carefully assessed both the potential benefits and privacy risks of this use case and believe that the substantial benefits to our community outweigh the minor risks. Specifically, our analysis showed _____. (See Data Benefit Analysis exercise below).

- **Differentiate between the IDS' legal, ethical, and equity-based obligations.**
  - Our IDS goes above and beyond basic legal compliance to protect your privacy.
  - We are committed to only using integrated data in ways that are ethical and equitable to everyone in our community.
  - Our choices about data and privacy are informed by legal, ethical, and policy guidelines relevant to our community, such as _____, _____, and _____. (For example, your city or state's Privacy Principles, relevant state or federal laws, or ethical codes of conduct).

B.3: Talking Points — Responding to others' privacy expectations

For many people, personal privacy is deeply emotional and its real or perceived absence may leave them feeling vulnerable, exposed, or out of control. This is why trust and transparency are essential to building successful and sustainable IDS, and why IDS must try to fully understand and appreciate their community's perspectives about how and when to use data appropriately. There may be a variety of reasons that community members support or object to a particular use case. Listening to community members' voices and responding to them are two different skills and workstreams, and IDS should learn to do both.

Key strategies and messages:

- **Understand that community expectations and preferences surrounding privacy are diverse.**
  - We know that privacy risks impact different groups in different ways, and we are prioritizing a variety of inclusive public engagement opportunities to be sure we are hearing from diverse voices.
  - We know that not everyone will agree about how data should or should not be used, and before we go forward we want to have a conversation about our community values and priorities.
  - It is important to our IDS that *this* community generally agrees with how we are proposing to use integrated data and feels comfortable with the process.

- **Anticipate pushback to data-driven initiatives.**
  - Feeling out of control – e.g., "Why can't I opt out," "Who decided that this was going to be good for me?" and potential responses:
    - The IDS' work is valuable because it is a snapshot of the entire community, and would be less effective and unrepresentative if some community members' information was not included.
    - Our privacy laws specifically permit this use of data, because our legislatures recognized the value of this kind of evaluation to improve government services.
    - Community members have a voice and will be included through our public engagement activities, and the final outcome will reflect that.
    - There is a data governance body that sets transparent policies and procedures for data use. The governance board is made up of _____ and our policies and procedures can be found here: _____.
  - Mistrust of research – e.g., "I don't want to be a guinea pig," and potential responses:
    - Using administrative data to evaluate potential solutions to community issues actually means we do not need to collect more data or conduct intrusive experiments to better understand our community.
    - Analysts using the IDS only receive aggregated and de-identified data so that researchers cannot identify particular individuals.
    - We have strict legal, procedural, and ethical standards to reduce the risk of harm to any individuals.
  - Concern about bias or issues of inequality – e.g., "This effort/data is biased against my community" or "this effort will exacerbate societal inequalities," and potential responses:
    - We recognize that some data may contain historic biases that can discriminate against or have serious impacts on our communities, and we are taking steps to ensure that we mitigate any such risks, such as conducting a disparate impact analysis.
    - Data can be a tool for revealing and addressing bias and discrimination that already exist in our community rather than a tool to exacerbate biases.
    - We have strict data quality standards and are working with leading domain experts, advocates, and community members to ensure our work respects their experiences.
  - Mistrust of institutions – e.g., "I don't trust the government" or "this is just more from Big Brother," and potential responses:
    - The IDS is an _____ organization [within/outside of] or state/local government, with strict oversight and accountability mechanisms.
    - The IDS has no connection to federal agencies or other entities outside our state/local government.
    - We are engaging in robust public engagement and involvement activities to ensure that the IDS is driven by our community members' priorities at every stage.

- **Anticipate pushback to privacy protection efforts.**
  - Innovation – e.g., "This [privacy safeguard] will stifle innovation," and potential responses:
    - Our IDS' policies are designed to give us the best of both worlds, so that we can maximize innovative data uses while sustaining the public's trust and protecting community members from harm.
    - Evidence shows that privacy protections play an important role in creating environments in which experimentation and innovation flourish.
    - Investing in appropriate privacy safeguards up front will build our community's trust and save us time and resources later, supporting future innovation.
  - Not my job – e.g., "I'm just a researcher/engineer/developer, I don't control how the data is used," and potential responses:
    - Protecting our community's privacy is everyone's responsibility. It is an important part of our IDS' values and our roles as public servants.
    - Our IDS is committed to protecting our community members' privacy by design and by default, and our technical and data experts are often our front-line responders to potential privacy risks.
  - Nothing to hide/public data – e.g., "If you have nothing to hide, then you shouldn't be concerned" or "But it's all public information anyway," and potential responses:
    - Privacy isn't about "hiding" information about yourself, it's about being in control of who has your information and what they can do with it. Even if you do not feel strongly about how your information is used, your data can have an impact on your friends, family members, neighborhood, and entire community.
    - Although administrative data is already being collected and used by public agencies, our IDS has a responsibility to protect the data and to consider additional risks that might arise when the data is combined in new ways.
  - Resignation – e.g., "I lost my privacy long ago and my opinion won't matter anyway" or "You don't really expect me to read another privacy policy, do you?" and potential responses:
    - It's important to our IDS that our community members know and approve of what we are doing with integrated data.
    - Instead of burying information in a privacy policy no one will read, we are committed to providing our community members with meaningful, inclusive public engagement and involvement with opportunities for everyone's voice to be heard.
    - As a member of our community, your opinions about data and privacy are important to us and we want you to be a part of our decision-making processes by joining/doing _____.

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.

B.5: Exercise — Elevator Pitch

An "elevator pitch" is a critical communication tool, intended to spark interest in your IDS or a particular use case. The goal is to prepare a concise, compelling introduction that anyone can understand within 20-30 seconds and that can form the foundation for many other communications. It may seem straightforward, but succinctly and persuasively articulating the goals of an IDS to a non-technical audience takes practice.

In one sentence, describe the goals of your IDS' latest use case for a stakeholder who is not familiar with you or your work. Even if you do not have a single concrete goal for how you will use administrative data, describe what you *hope* to accomplish. Be specific, but to the point. Use this opportunity to communicate the *top-level* benefits and values of your efforts. Avoid highly technical details or jargon.

For example:

- *Too technical:* We integrate administrative data in a centralized repository to evaluate the impact of state-supported education programs for at-risk students' attendance outcomes.
- *Better, but still too detailed:* We combine administrative data from multiple agencies to better understand how successfully our schools are supporting children at risk of educational failure.
- *Best:* We link data from public agencies to help our schools better serve the most vulnerable students in our community, both in and outside of school.

ELEVATOR PITCH

Once you've drafted your pitch, try it out, then ask friends, family, and colleagues in other departments to evaluate your performance. Have several IDS colleagues go through the same exercise, and distill the results into a high-level message that everyone is comfortable sharing publicly. IDS' elevator pitches don't need to be identical, but they should be consistent.

B.6: Exercise — Advanced Elevator Pitch

Once your IDS has agreed on a basic elevator pitch, you can begin to adapt it to more specific audiences. The following series of exercises are intended to help you refine your core ideas in a variety of circumstances throughout the IDS and stakeholder engagement lifecycle:

- You get a call from a concerned lawmaker who wants to know what you are doing with the IDS. The lawmaker is neither supportive nor critical yet, but needs to quickly grasp the effort's value and ability to safeguard individual privacy. Answer in one sentence:

- The senior official of your agency summons you to their office and asks you to summarize the IDS and its goals. This official appreciates your agency's mission, structure, and resources, but is not deeply versed in the day-to-day of your work. Answer in three sentences or less:

- Your press office receives a press inquiry that asks for a quote from you that will fit in a news story about why the IDS is positive for the community. This quote will be offset in the story by critiques from privacy organizations. Answer in three sentences or less:

- You attend a public hearing about the IDS, and a concerned citizen and public advocate is hyper-concerned about privacy and distrustful of how your IDS will safeguard personal data. Respond to their concerns in five sentences or less:

- An agency participating in the IDS hires new legal counsel, who raises concerns about the organization taking on privacy and security risks and wishes to withdraw the agency's data from the IDS. Briefly respond to the counsel's concerns:

- You receive an email from a data scientist at another local agency (that does not yet participate in the IDS) requesting access to the IDS' data for an important internal project. Briefly respond to this request:

B7: Exercise — Data Benefit Analysis

Maximizing the potential of an IDS use case requires evaluating not only the risk but also the benefits of integrated data. The privacy risks should be articulated through a *Privacy Impact Assessment*. To account for the unique benefits of integrated data, however, we recommend conducting a *Data Benefit Analysis* as well.

Using this guide to *Benefit-Risk Analysis for Big Data Projects,* assess *in writing* the anticipated benefits and risks of each IDS use case and weigh them against each other. This includes specifying:

- What are the potential benefits of your IDS or IDS use case?

  _____

- What are the potential privacy risks of your IDS or IDS use case?

  _____

- Who are the potential beneficiaries of your IDS or IDS use case?

  _____

- Whose privacy is potentially at risk because of your IDS or IDS use case? (Is this the same group that would benefit from it?)

  _____

- What is the anticipated size or scope of the benefit of your IDS or IDS use case?

  _____

- What is the size and scope of the potential risk of your IDS or IDS use case?

  _____

- What is the likelihood that the benefit will occur?

  _____

- What is the likelihood that the risk will occur?

  _____

- What impact will anticipated mitigation strategies have on the potential benefits?

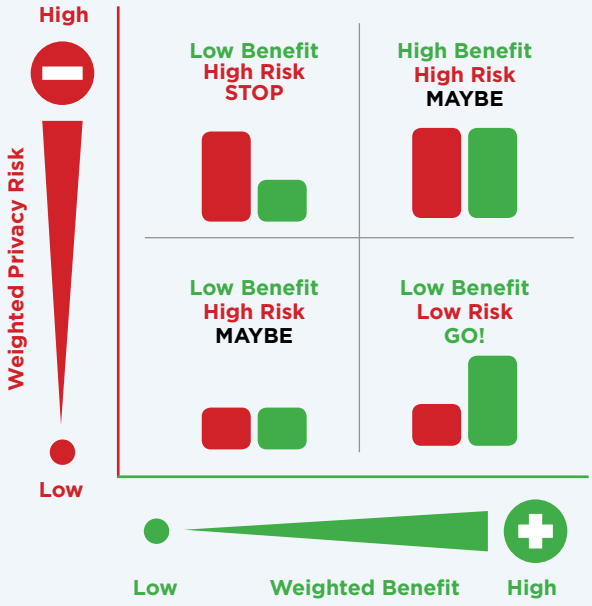
  _____

  _____

  _____

- What impact will anticipated mitigation strategies have on the potential risks? How do the weighted privacy risks and the weighted benefits compare?

  Circle one: **STOP** / **MAYBE** / **GO**



APPENDIX C: ENGAGEMENT WORKSHEETS, CHECKLISTS AND SAMPLE MATERIALS

C.1: Worksheet — Strategic Engagement Planning

1. What are our objectives for this engagement?

IDS planning teams must agree on what you want to achieve by engaging stakeholders around data and privacy issues. This may require several rounds of discussion, background research, and/or informal liaising with internal or external stakeholders.

Examples of possible objectives for an IDS privacy stakeholder engagement:[31]

- Understand local needs and wants around data and privacy
- Set research priorities
- Find agreement on the purpose and direction of a particular IDS or use case
- Promote active citizenship and a wider circle of responsibility for decisions and actions
- Encourage local buy-in and ownership in the IDS and develop social license to use administrative data
- Defuse conflict situations around data and privacy before they impede progress

Tips:

- Objectives may be broad or specific, depending on the organizational and community culture of your IDS. If internal buy-in for the engagement is still necessary, consider drafting objectives that are "SMART": Specific, Measurable, Assignable, Realistic, and Time-related.[32]
- Name your IDS' guiding principles up front. If transparency and an emphasis on racial equity are guiding principles, then engagement activities will be fundamentally different than, for example, another IDS that has "agency benefit" as a guiding principle.

2. What is the environment for this engagement?

It is important for IDS planning teams to explore the personal, organizational, and topical factors that may influence the engagement environment itself. Where an unprepared IDS might find their activities derailed by interpersonal conflicts between stakeholders, logistical hurdles, or cultural misunderstandings, for example, a more prepared IDS could anticipate or avoid such obstacles.

This may require several rounds of discussion, background research, and/or informal liaising with internal or external stakeholders, especially those who have participated in previous stakeholder engagement activities.

Issues to consider for particular IDS engagements include[33]:

- **Previous/other engagements:**
  - Have there been any previous data integration efforts within your community on similar issues, and what was the outcome?
  - If yes, did the data integration efforts include stakeholder or community engagement? And if so, what was the outcome?
  - Are there any concurrent engagement activities by other groups with your stakeholders, and how are those progressing?

- Is there a history of mistrust within this community towards any particular government agencies and/or partner institutions?
- Are there rules or expectations that discussions, attendance, or other notes about engagement processes will be made public, kept confidential, or be subject to other standards (e.g., "Chatham House Rule,[34]" subject to Freedom of Information requests, etc.)?

› **Stakeholders**

- Is this the first time any anticipated stakeholders have engaged in this kind of participatory public process?
- How technically sophisticated or digitally literate are your anticipated stakeholders?
- Do any of your anticipated stakeholders have specific physical or cultural needs that should be accommodated in physical and digital spaces (e.g., literacy, accessibility, language)?
- Do any anticipated stakeholder groups have a history of antagonism towards other stakeholders or IDS representatives around these issues?
- Have any anticipated stakeholder groups traditionally aligned with each other or IDS representatives around these issues?

› **Issue sensitivity:**

- Is there any history of this community's privacy being violated by state or local government? By researchers?
- Is there any political sensitivity around this topic? Are there any social or economic issues that the community has dealt with related to this use case?
- Are there any other dominant political issues that are top-of-mind for your community, and that might distract from a conversation about data and privacy?

Tips:

› Consider the diversity of participation experience amongst the identified stakeholder groups. Those with more experience may have skills and confidence to dominate proceedings, while those with the least experience may need more support navigating the process or having their voices heard.

› Consider the cultural diversity of participants which may affect, for example, people's willingness to meet all together (e.g., men and women together), and/or affect the way different participants are used to debating in public with others (e.g., those with formal committee experience may expect a chair and formal debating procedures).[35]

3. What are our resources for engagement?

Successful stakeholder engagement activities—particularly around privacy, which can which can require both deep technical skills and empathy—require adequate time and resources. By being honest and specific about these factors up front, you will be better prepared to efficiently leverage your stakeholders' input.

This may require several rounds of discussion, background research, and/or informal liaising with internal or external stakeholders.

In determining the required resources for your engagement exercise, items consider include:

› **Timeline:**

- What is the minimum/maximum time this engagement is anticipated (or allowed) to take?
- How much time will each engagement activity take?
- How much time (if any) will be needed for internal processing between each engagement activity?
- How much notice or time to mobilize (if any) will you need to give potential participants before each engagement activity?
- How many participants do you anticipate involving at each engagement activity?
- How much education or level-setting will you need to do with stakeholders before each engagement activity?
- How complex will this IDS/IDS use case be? How consequential will this IDS/IDS use case be on the community? (Typically, the more complex or consequential, the more time should be set aside for engagement.)

- **Staff:**
  - Do you or partners have staff with meeting facilitation experience?
  - Do you or partners have staff with participatory engagement experience?
  - Do you or partners have staff with subject matter expertise in data, privacy, and security?
  - Do you or partners have staff with communications and public outreach experience?
  - Do you or partners have staff who can offer technical and logistical support for engagement activities, including events?
- **Budget:**
  - Will communications and outreach efforts need to be funded?
  - Will informational materials need to be created, published, or printed?
  - Will in-person events need to be planned? Consider, if applicable, costs for renting or using physical spaces, seating and tables, audio/visual, food, childcare, etc.
  - Will digital/virtual events need to be planned? Consider, if applicable, costs for web development, streaming, or advertising.
  - Will external experts or consultants need to be engaged or reimbursed for travel?
  - Will any accommodations need to be made for persons with disabilities?
  - Will any participants be compensated for their time?
- **Capacity for change:**
  - What is the decision-making environment for this IDS/IDS use case? Who has final authority? (For example, IDS governance board, an agency head, a political leader, a community oversight board).
  - How committed are internal leadership to meaningful/active stakeholder engagement (i.e., stakeholder input will have some material impact on outcomes)
  - What aspects of the IDS/IDS use case are open to stakeholder influence?
  - What aspects of the IDS/IDS use case are non-negotiable?

Tip:

- It is critical that the IDS clearly establish what aspects of the IDS/IDS use case can realistically be affected by stakeholders' participation. If stakeholders are given unrealistic expectations or dedicate significant time and energy to a process that did not yield any results, trust and goodwill for the IDS will be eroded. If an IDS is designed so that stakeholder input does not matter or if there are insufficient resources to follow through on the engagement team's promises, there is no point in going further with the engagement process.

C.2: Worksheet — Stakeholder Mapping

1. Identify your potential stakeholders

AISP's Expert Panel Report on Data Governance[36] recommends considering IDS stakeholders from three categories:

- **Core stakeholders,** without whose engagement the IDS cannot achieve success
  - Data owners and contributors (directly contributing, or facilitating access)
  - Funding sources (government, private foundations, other)
  - Public agency leadership and key elected officials
- **Other direct stakeholders,** whose engagement can help facilitate (or impede) IDS success but who are not in the core group
  - Data users (researchers, advocacy groups)
  - Technical experts (legal, data technology, security, research methods, fiscal)
  - Privacy advocates
  - Advocates for vulnerable populations and communities
- **Other stakeholders,** who can broaden interest of the IDS and deepen its constituencies
  - Business groups
  - Good government groups
  - Other citizen and public interest groups

In order to make sure no one is overlooked, or to narrow in on specific people or groups within those categories, consider these additional questions:[37]

- Who will be representing the interests of the individual community members whose administrative data is being used?
- Which people or organizations will be affected by the results of your IDS or specific IDS use case(s), now and in the future?
- Which people or organizations are influential on this issue at the local, state, national, or international level?
- Who is influential within your particular area, community and/or organization?
- Who can obstruct a decision if they are not involved (individuals, funders, political leaders, oversight groups, etc.)?
- Who has been involved in this issue in the past?
- Who has not been involved in past engagements, but should have been?
- Are there any barriers to engagement that may be/have been deterring some stakeholders?
- Who else would your current stakeholders invite to participate?

Tips:

- **Representativeness.** Some groups of stakeholders are more difficult to reach than others, and are thus often the least likely to be represented in policymaking processes. IDS should be creative and go the extra mile to be inclusive, so as to provide a more balanced picture of the community within the engagement process.
- **Opposition.** Stakeholders should not be excluded simply because they are likely to oppose the IDS or a specific IDS use case. In fact, potential challengers are some of the most important voices to hear from if an engagement process is to be representative and legitimate. Bringing potential opponents into the process can also give them a sense of buy-in and ownership, or at least an appreciation for the good faith of the other participants.

2. Assess your potential stakeholders' interests

Next, assess whether or not the potential stakeholders you have identified are likely to support the IDS/IDS use case, or whether they are likely to be uninterested or unable to participate in the engagement process. Importantly, assess ***why or why not,*** and ***in what ways,*** each group is likely to advance or impede the engagement and the process. Consider the possible range of interests—both positive and negative—of each group, such as:

- Interest in improving service delivery, fostering research, or advancing policy goals
- Making the case for additional resources or identifying opportunities for savings
- Strengthening governmental administration, accountability, or efficiency
- Potential of being embarrassed about poor data quality, programmatic problems, or exposing unmet needs/new costs
- Potential burdens of cooperation
- Inertia and organizational culture
- Privacy and security
- Turf wars
- Legal compliance concerns

Tip:

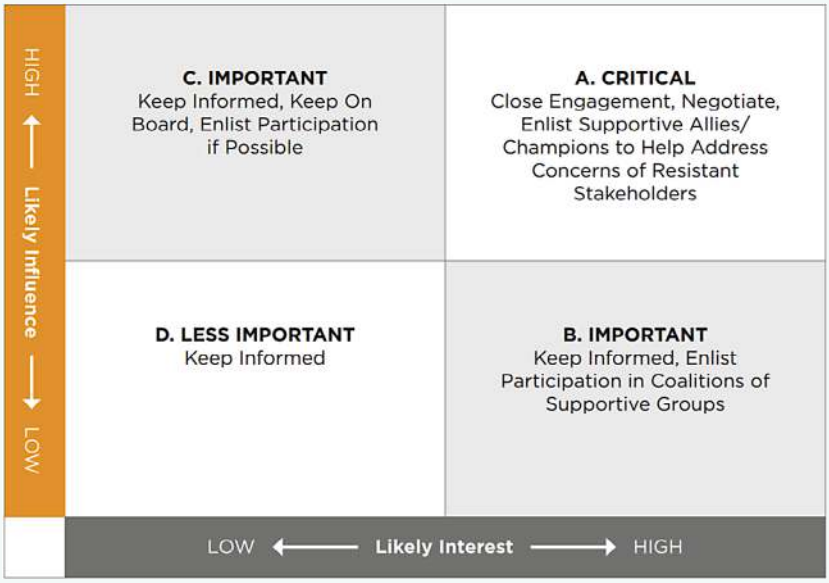
- **Giving back value.** Many stakeholder groups have even more limited resources to participate in public engagements than IDS have to put them on. Discuss with participants what they want to get out of the process or what hurdles might limit their participation.

For a sample stakeholder analysis, see C.10 in this Appendix.

3. Prioritize your key stakeholders

Finally, prioritize your key stakeholders based on the information above and finalize the group of stakeholders who you intend to formally engage.

To do this, it is useful to think along two dimensions, as illustrated below. Powerful stakeholders with strong interests (quadrant A) demand the most attention.



Tips:

- **Finding Early Allies.** Those who are likely to be advocates for the IDS should be engaged early and encouraged to help address the concerns of other groups that may be influential but less supportive.
- **Champions.** When dealing with internal stakeholders, having dedicated "champions" can be an effective way to keep an IDS visible and relevant across several departments or organizations.
- **Transparency.** Determining which stakeholders actually participate in an engagement can become contentious, and so it is helpful to make the selection criteria as transparent as possible.
- **Group size.** Although diversity in stakeholder perspectives is important, an overly-large group may be less effective in reaching consensus or navigating complicated discussion points. The size of the group should reflect the breadth and sophistication of the participants, the complexity of the use case and engagement, and consequence of the IDS' activities.

* This worksheet builds on material developed in the *AISP Expert Panel Report: IDS Governance: Setting Up for Ethical and Effective Use,* available at https://www.aisp.upenn.edu/wp-content/uploads/2016/07/Governance.pdf

C.3: Worksheet — Pre-Engagement Planning

1. Prepare answers to basic questions on process and substance

Informing *and* engaging stakeholders at the same time is a challenge. Ensure that enough time is set aside to bring everyone up to speed on the basics of how data could be used and protected, particularly with non-technical stakeholders.

IDS should be able to communicate to stakeholders (at least preliminarily) about:

- **Personnel:**
  - Who will have ultimate decision-making authority?
  - Who are the subject matter experts?
  - Who will be stakeholders' primary point of contact?
  - Who else will be participating in the engagement exercise?
- **Process:**
  - What aspects of the IDS or use case will stakeholders be able to influence?
  - How long is the engagement intended to last?
  - Will discussions be held in person or online?
  - Will discussions, attendance, or other notes be made public, kept confidential, or other (e.g., "Chatham House Rule,"[38] subject to Freedom of Information requests, etc.)?
- ***Proposed* goals of the IDS:**
  - How will the IDS or IDS use case benefit the community?
  - What questions will the IDS or IDS use case answer?
  - What policy outcomes could this IDS or IDS use case lead to?
  - How likely are those outcomes?
  - How does this IDS or use case fit into the mission or agenda of other internal stakeholders or key elected officials?
  - How and when will results be shared?
- ***Proposed* privacy and ethical considerations:**
  - What legal or ethical codes will apply to your use of administrative data?
  - What are potential risks to individuals' privacy and civil liberties?
  - Could the data reflect biases (including racial or socioeconomic)?
  - How (besides this engagement) has the IDS incorporated community input and expectations around data and privacy?
  - Which communities will be most likely to benefit from the IDS or use caset?
  - Which communities could be excluded or harmed?
- ***Proposed* data and privacy protocols:**
  - What specific data elements would the IDS or IDS use case include?
  - How (besides this engagement) will impacted communities be given notice about how their data is used and protected?
  - Who will have access to the IDS's data, and how will they be vetted and supervised?
  - How long will the data be retained?
  - How will data be secured?
  - What if there is a data breach?
  - How will data be de-identified?
  - What will happen to the data after the IDS or use case ends?
  - What oversight or remedies might be offered if privacy is violated?
  - Will other government entities have access to the data (e.g., law enforcement, federal agencies, etc.)?
  - What efforts will the IDS take to account for systemic data biases?

Tips:

- Do not arrive at an engagement activity with firm and finalized plans about how data will be used and protected, but also do not arrive with a blank slate. Engagement leaders can strike a balance by providing clear and detailed proposals for how the IDS or use case *might* progress for stakeholders to respond to, as well as by providing time for stakeholders to suggests their own alternatives.
- Make this information available to the public beforehand, in a variety of formats, and invite questions in advance of your engagement activities.

2. Identify what informational or discussion materials you will need

Particularly when bringing stakeholders together to discuss issues like privacy and appropriate data use, providing baseline informational materials about the IDS and its proposed use case is critical to ensuring everyone is on the same page and can meaningfully participate in your engagement activity.

Based on your answers above, identify what kinds of substantive materials will need to be generated to ensure a productive engagement. Items to consider include:

- Proposed scope of your IDS or use case (research questions, methodology, budget, timeline, metrics of success)
- Engagement plan (timeline, activities, decision-making, results)
- Communications materials (FAQs, one-pagers, infographics, videos, visual aids)
- Technical explainers (law, data, security, privacy, research methods)
- Bibliographies, literature reviews, or related academic works
- Biographies and contact information (IDS staff, researchers, invited experts, engagement participants)
- Expert opinions, reports, or impact assessments (privacy, ethical, environmental, de-identification)

Tips:

- Multiple versions of informational documents may be necessary, depending on the breadth of the engagement, language or literacy differences among participants, and the technical sophistication of different stakeholders.
- Consider inviting subject matter experts to translate technical information into plain language that everyone can understand.

C.4: Worksheet — Convening Stakeholders

1. Deciding when to engage

Generally, IDS are encouraged to engage select groups of stakeholders as early and as often as is practical. While engagement for general IDS efforts should be on-going, it many also be necessary to conduct engagement activities for specific IDS use cases. One easy way to think about when to create engagement opportunities is to think about a typical integrated data lifecycle, and where along it stakeholders' insight would be most significant:

IDS Use Case Lifecycle

1. **IDS use case conception and formulation.** Engagement at this stage is particularly valuable (to project teams) and meaningful (to stakeholders), as clear input can easily shape the entire effort and community ideas and priorities can be immediately reflected. Understanding and respecting stakeholders' views around data and privacy *before* personal data is obtained is essential to responsible research.
2. **Secure legal agreements for integrating data.** Outside legal or policy experts may be engaged at this point to review proposed data use agreement terms or serve on oversight panels. Internal agency leadership or champions may also have strategic input at this stage.
3. **Cleaning and linking data.** Data owners, data scientists, and technical experts from both outside and within the state/local government may be helpful here, for example, in staffing a disclosure review board to limit re-identification risk or evaluating the effectiveness of data linking protocols. Typically, non-technical stakeholders would not be engaged at this stage.
4. **Analyzing the data.** At this stage, subject matter experts, advocates, and data scientists may be brought in to help review the analysis or test for disparate impact. A more diverse group of experts and community representatives, particularly from traditionally under-represented and/or marginalized groups, may also be considered at this stage.
5. **Disseminating findings.** Community organizers and advocates, public officials, agency leaders, business leaders, and a wider range of stakeholders can have real impacts at this stage by leading broader discussions focusing on potential policy recommendations arising from the IDS's findings. External community stakeholders may be particularly effective in making the IDS's findings relevant and accessible by traditionally overlooked groups within the community.
6. **Wrap up and review.** Any stakeholder who participated earlier in the process should have an opportunity to close the loop by evaluating the effectiveness of the use case and of the engagement itself.

Tips:

- It may not be practical or necessary to engage every (or any) stakeholder at every phase of the data lifecycle. While some stages, like defining your use case and research questions, or sharing your findings, lend themselves to a broad range of stakeholder inputs, more technical stages, like securing legal agreements or cleaning and linking your data, may be better suited to smaller engagements with groups of content specific experts.
- Consider balancing out a phase with weaker engagement by increasing efforts at another stage (e.g., spend less effort engaging on data linkage and more on use case conception and formulation).
- Recurring engagement activities help stakeholders feel invested in the IDS and often improves the quality of their input; however, participation also has an opportunity cost for stakeholders and too many engagement requests may exhaust even the most dedicated supporter.

2. Deciding what engagement activities are the best fit for your IDS and use case

There are as many ways to engage stakeholders as there are opportunities to do so, but not every method of engagement is a good match for every stakeholder.

You can learn what is the right fit for your set of stakeholders through experience, or by asking others who have hosted engagement activities within your community. Factors to consider might include:

- **Structured/unstructured** – formal processes may be more comfortable for some stakeholders, while others may prefer loose and informal convenings.
- **In person/virtual** – some people may work best face-to-face, while others may desire the anonymity or unstructured response times of an online platform.
- **Active/passive** – more active engagement methods will create more meaningful experiences for stakeholders, but may be more expensive or time-consuming to provide.
- **Group size** – larger stakeholder convenings may allow for more perspectives to be included at once, but may also make it more difficult to manage the flow of conversation.
- **Stakeholder priority** – stakeholders with more interest or more influence in the IDS or use case might benefit from more active engagement opportunities than those with less interest or influence.
- **Cost** – depending on you and your partners' resources (such as access to physical spaces or web hosting), costs may vary significantly between in-person and virtual activities.
- **Timeline** – timelines for these activities may vary widely, but in particular consider how many times the activities will need to be held; how long logistical details will take to secure; how much notice participants will need to ensure sufficient attendance; and how long will be needed for internal approvals during planning and follow-up.

Tips:

- Strive to create opportunities to *empower, collaborate, or involve* your stakeholders, rather than simply *consulting* or *informing* them of what you are doing. See diagram in the *Engaging Stakeholders around Integrated Data* section for more.
- See the diagram in Step 4 of the *Engaging Stakeholders about Integrated Data* section for examples of specific engagement activities.

3. Engaging Inclusively

Engagement planning teams should proactively build capacity to host engagement activities that appreciate the implications of race, language, culture, and socioeconomic status on stakeholder engagement. Considerations for culturally diverse and inclusive spaces, platforms, and materials include:

- **Language and literacy,** such as by using bilingual facilitators, providing translators, or providing for oral participation.
- **Food,** such as providing vegan, halal, or kosher meals.
- **Location,** such as by meeting near public transit or in spaces familiar to traditionally marginalized or underserved populations.
- **Time,** such as hosting multiple engagements to allow shift workers or students to participate or accommodating prayer times for religious participants.
- **Childcare,** such as by providing childcare during in-person meetings.
- **Incentives,** such as by providing free food and drinks at meetings, gift cards for filling out surveys, or compensating participants for their time and knowledge.
- **Appeal,** such as by increasing use case relevance and impact on particular community groups.
- **Power dynamics,** such as by offering meaningful decision-making authority over IDS and use case design and direction.
- **Accessibility** (physical and digital),[39] such as by providing ADA-compliant physical and digital spaces or providing assistive technologies for those with physical or mental disabilities.

Tips:

- As you build your IDS' capacity for cultural responsiveness, resources like the City of Seattle's Inclusive Outreach and Public Engagement Guide[40] and the University of Washington Tech Policy Lab's Diverse Voices Guides How-To Guide[41] may be helpful.

4. Engagement Matrix

It may be helpful to visually brainstorm or document potential engagement opportunities in a matrix like the one below, keeping in mind that no two IDS engagement strategies will look alike. Your IDS should use the combination of engagement activities that best fits your needs based on the scale, scope, and context of your data-driven activities, as well as the time and resources available to you and your stakeholders.

	← *more active* ---------- *more passive* →				
	Empower	**Collaborate**	**Involve**	**Consult**	**Inform**
Use case conception and research formulation					
Securing legal/partner agreements					
Cleaning and linking data					
Analyzing data					
Disseminating finding					
Wrap up and review					

Tips:

- Strive to create opportunities for more active participation when possible.
- Remember that you do not necessarily need to engage all stakeholders at all stages in the IDS lifecycle, and can balance out more passive engagement at some stages with more active engagement activities at others.
- To see a sample, hypothetical IDS use case illustrated in a similar template, see Appendix 1 in the ADRF Network's Report on Communicating about Privacy and Security (developed in collaboration with FPF, AISP, and other administrative data users).[42]

C.5: Worksheet — Closing the Engagement

At this stage, IDS engagement teams should review the engagement efforts and record:

- Any decisions or recommendations made by stakeholder groups
- Key issues and proposed solutions raised by stakeholders
- Points of agreement and disagreement between stakeholders
- Any additional feedback from stakeholders (in follow-up conversations, surveys, or other outreach)
- Any other important factors or perspectives that arose during the engagement activities

It is almost certain that your stakeholders will have held conflicting perspectives on how best to use and integrate administrative data and to safeguard individual privacy, so IDS leadership will still need to do the hard work of deciding how to respond to those varied perspectives and policy choices. Keeping in mind the decision-making environment and resources that you identified in the initial engagement scoping exercise, your IDS must decide whether to take action on **all, some, or none** of your stakeholder's inputs.

It is important to recognize that successful stakeholder engagements involve flexibility and compromise, and that there may not be one perfect solution that meets everyone's needs. In these cases, IDS should seek to be as transparent as possible about how and why certain decisions were made and remain open to re-examining those choices in the future. Participants who may be disappointed in the outcome should be offered opportunities to stay involved.

Tips:

- How policy decisions are made will depend on the particular IDS' governance and culture, as well as relevant legal, ethical, and policy guidelines. In all cases, however, the reasons for the ultimate decision should be documented and made available to interested stakeholders.
- Where stakeholder perspectives diverge, IDS may need to make tough choices. When stakeholders do reach a common consensus, IDS leaders should respect that input and strive to abide by it as much as possible.

C.6: Checklist — Meeting Facilitation

Use this checklist to help facilitate active, inclusive stakeholder discussions on responsible data use and privacy.

TONE

- ☐ Open discussions with a friendly, welcoming tone. End on a positive, optimistic note.
- ☐ Speak with simple and direct language.
- ☐ Display energy.
- ☐ Message that diversity of voices is an asset.
- ☐ Be attentive while others are speaking; participants should be the center of attention, not facilitators.
- ☐ Direct questions to experts or other participants, to avoid the impression of being the authority in the room.
- ☐ Stay neutral; facilitators should not be defensive or argumentative.

SETTING THE STAGE

- ☐ Be clear who is running the meeting and what its goal is, including what parts of the IDS use case can and cannot be impacted by stakeholders' input.
- ☐ Introduce all participants.
- ☐ Let everyone know the meeting rules (e.g., when there will be opportunities to speak, what is on and off topic, whether the meeting will be recorded and how such recordings will be used, etc.).

MANAGING DISCUSSION

- ☐ Check in with participants to see how the discussion is going.
- ☐ Keep track of key ideas. (A white board, flip pad, or digital tracker may be helpful).
- ☐ Have a range of discussion tools on hand, in case one approach doesn't work or a new direction is needed.
- ☐ Assertively (but not aggressively) manage conflicts so that everyone has an opportunity to be heard and the discussion stays on topic.
- ☐ Keep the discussion on topic, and have a way to capture off topic comments so that they can be addressed at another time.
- ☐ Bring closure to the discussion, and end with clear steps for the next meeting.

ENCOURAGING DISCUSSION

- ☐ Keep explanations as simple as possible; avoid acronyms and technical terms.
- ☐ Treat all participants as equals.
- ☐ Don't let a few people dominate the whole discussion.
- ☐ Solicit comments from those who haven't spoken yet, or who might have been spoken over.
- ☐ Consider ways to encourage a range of participants, such as written comment/question cards, small group break outs, or one-on-one outreach.
- ☐ Allow silence to be comfortable. If there is no response to a question, wait 20-30 seconds before prompting or restating the question.
- ☐ Tell participants that all perspectives are welcome, and that different points of view are valuable.

FOLLOW UP

- ☐ Ensure that participants feel ownership for what has been achieved.
- ☐ Ask for feedback about the meeting process and use it to improve future meetings.
- ☐ Follow up with those who might be disappointed with decisions you made and encourage them to stay involved.
- ☐ Prepare and distribute a meeting summary, including any decisions, action items, and future meetings, and identify a specific contact person for participants to reach out to with additional questions or comments.

C.7: Checklist — Public Engagement Meeting Planner

Having well-thought-out meetings requires a lot of preparation. The following checklist will help you work through who, how, and what your meeting will address.

TARGET ATTENDEES / STAKEHOLDERS

- ☐ Community members
- ☐ Community leaders
- ☐ Government leaders
- ☐ Civic groups
- ☐ Other _____

GETTING THE WORD OUT

- ☐ Social media
- ☐ Email
- ☐ Website
- ☐ Notification tree (using contacts to spread the word)
- ☐ Electronic invitation system (allows for collection of RSVPs)
- ☐ Existing publications (e.g., newsletters or newspapers)
- ☐ Posters or flyers

INVITATION MESSAGING AND FORM

- ☐ Clear, concise language written for the potential audience rather than bureaucrats or lawyers
- ☐ Meeting expectations - What will the audience participate in and what can they learn?
- ☐ Contemplate and address in advance the potential attendee's question of why they should attend
- ☐ Emphasize value of community member input
- ☐ Double check the date, time, and location information
- ☐ Consider whether supplementary materials will be distributed with the invitation

WHEN

- ☐ Weeknight vs. weekend
- ☐ Morning, afternoon, or evening
- ☐ Do you want to send a message of inclusiveness? If yes, carefully consider your timing.
- ☐ Is there a holiday (religious or secular) that may conflict?
- ☐ Can this meeting be hosted multiple times?

FORMAT CHOICE

- ☐ Lecture
- ☐ Interview
- ☐ Mainly Q & A with short introduction
- ☐ Workshop or other interactive format
- ☐ Public hearing or debate
- ☐ Open house
- ☐ Facilitated learning
- ☐ Small group discussion or focus group
- ☐ Small group advisory board or expert panel
- ☐ Other_____

AGENDA SPECIFICS

- ☐ How much time do you have?
- ☐ How much time do you need?
- ☐ How important is audience participation and engagement (relates to timing, structure, and content)?
- ☐ How do you intend to facilitate audience participation?
- ☐ Have you solicited participation from civic leaders or other potential stakeholders?
- ☐ Are there opening statements or speeches or talking points?
- ☐ Consider anticipating and addressing audience questions and concerns from the start (e.g., cybersecurity, data ownership, data access, transparency, etc.)
- ☐ Do you have a presenter who can address technical questions?
- ☐ Consider key topics and narratives to engage the audience

RULES OF ENGAGEMENT

- ☐ If you are recording or transcribing the event, have all participants been notified? Will those materials be made available publicly, or could they be compelled through a Public Records Request?
- ☐ If the event is all or partially off the record, what will participants be able to relay after the event? For example, if the event will be held under the "Chatham House Rule," where attributing specific statements or points of view to any participant or class of participant is not permitted.[43]
- ☐ What will be considered on and off topic, and how will off topic discussions be handled?
- ☐ Will press be present at the event?
- ☐ Who will be permitted to speak and when? (E.g., time and turn restrictions, and why they are in place)
- ☐ Allow for questions in advance or in lieu of attendance?
- ☐ Do you have/need a code of conduct?

WHERE AND HOW: IN-PERSON MEETINGS

- ☐ Who will host and is there a strategic reason to have a certain host? A government or academic building may inspire confidence for example and illustrate partnerships. A community building, on the other hand, may demonstrate a commitment to inclusiveness and collaboration.
- ☐ Event space accessibility, capacity, and comfort
  - Is the space big enough? Are the temperature and lighting comfortable? Are there bathrooms, trashcans, and recycling nearby?
  - Is the space convenient for your audience to reach? Is it near public transit? Is there sufficient (free) parking?
  - Can you go to your audience rather than having them come to you?
  - What are the costs involved?
  - Is the space accessible to persons with disabilities? (Ramps, elevators, appropriate spacing between and at tables for wheelchairs, etc.)
  - Do you need tables, chairs, or a podium? How will they be arranged in the room?
  - Do you need signs or staff to direct people around the space?
  - Do you need to provide childcare?
  - Are you serving food or drinks?
  - Will there likely be language barriers? Do you have plans to provide a translator and/or translated materials?
  - What security needs or emergency plans do you have in place? (E.g., first aid kids, fire escape routes, power outage contingencies, etc.)
- ☐ Technology
  - Is the available technology sufficient? (Audio/visual or display technologies, microphones, computers, projectors and screens, laser pointers, etc.)
  - Is there Wi-Fi or wired internet connectivity strong enough for participants and/or presentations?
  - Should the event be fully or partially live streamed or video recorded? (If so, audience members participating in-person should also use microphones).
  - Should questions come from a virtual audience (e.g., via social media, email, or video conferencing)?

WHERE AND HOW: VIRTUAL MEETINGS

- ☐ What tools or capabilities are important in your digital space or platform?
  - Storing and presenting information
  - Annotation and comment tools
  - Real-time editing
  - Polls
  - Video streaming or playback
  - Social media plug-ins
- ☐ What additional tools will be needed to achieve those capabilities for participants and/or presenters?
  - Microphones and web cameras for all (consider quality vs. cost tradeoffs)
  - Wired vs. wireless connection for participants
  - Ability to remotely mute participants if background noise becomes disruptive
  - Anonymous post-event survey or evaluation forms
  - Digital copies of all event materials
  - Digital security and emergency plans (in case of a sudden surge of participation or disruption in Internet service)
- ☐ Is the digital space accessible? (e.g., closed captioning, keyboard commands, color blindness considerations, etc.)
- ☐ Will participants need to register or sign-in to the virtual meeting space or platform? What level of authentication/verification will be required? (Allowing anonymous participation may drive engagement up, but might open the process to trolling).
- ☐ Do you have an appropriate privacy policy and terms of service in place for attendees? (Be careful about repurposing boiler plate language from other websites, which may include broad rights to share personal data or limit users to arbitration).

SUPPORT AND SUPPLIES

- ☐ Discussion facilitators
- ☐ Assistants — greeters, note takers, technical or physical support staff, accessibility support (translators, sign language interpreters, etc.)
- ☐ Subject matter experts and IDS representatives
- ☐ Sign-in and contact sheets (useful for follow up, but keep in mind that some attendees may prefer to be anonymous)
- ☐ Name tags and/or tent cards
- ☐ Agendas (with estimated times)
- ☐ Informational and discussion documents, presentations, and visual aids
- ☐ Staff or speaker biographies and contact
- ☐ White boards, easels, or other interactive discussion tools
- ☐ Anonymous post-event survey and evaluation forms
- ☐ Notepads and writing tools for participants
- ☐ Directional signs
- ☐ Microphones, computers, and other display materials
- ☐ Recording device, if applicable

FOLLOW UP

- ☐ Survey
- ☐ Social media
- ☐ Blog
- ☐ Direct contact
- ☐ Email
- ☐ Who is responsible for follow up and follow through?
- ☐ Will there be additional meetings?

C8: Sample — Stakeholder Meeting Agenda, Privacy Specific

Distinct engagement and communications goals will require distinct strategies and meeting agendas. The sample agenda below is designed to guide a privacy-specific discussion during the development stage of IDS building, but could be modified for other purposes (e.g. to introduce a new potential use of the IDS). Regardless of purpose, be mindful about balancing listening (during informational presentations/level-setting) and more active speaking opportunities.

Recommended meeting length: 1-2 hours

Recommended attendees: key IDS stakeholders, including community members and community-based organizations

STAKEHOLDER PRIVACY MEETING SAMPLE AGENDA

AGENDA ITEM	RECOMMENDED LENGTH	NOTES
Registration & Refreshments	15–30 minutes	
Welcome & Introductions Who are we? Why are we here today?	5–10 minutes	Led by a core IDS planning team member with strong communications skills. Introduce all participants, including audience members.
Introduction to IDS What is an IDS? About our IDS — who are we, where do we come from, who funds us, when did the IDS form? What are our IDS' guiding principles? Our IDS' goals — what specific problems are we trying to solve? Who are our stakeholders? (Include community members)	5–15 minutes	Use active and specific language. If this is the first or second time participants have heard about the IDS, spend more time describing your goals, guiding principles, and structure. If stakeholders are already familiar, spend less time here. Provide written FAQs or other introductory materials to supplement the presentation and provide additional detail.
Data Privacy and Governance Why privacy matters What are IDS privacy risks? How we protect (or propose to protect) data privacy: ▪ Committee structures (governing board, data oversight committee(s)) ▪ Data License Review Process (analyst credentialing, de-identification standards) ▪ Data governance and data security (legal, technical, procedural) ▪ Response protocols (in case of a breach/incident) Clarifying Q&A	10–20 minutes	This section should be short and concise — it is intended to introduce data privacy issues and tools, which will be more deeply discussed during the engagement activity. Provide time for clarifying questions if participants are confused about specific points, but hold in-depth discussions for the engagement activity. Consider inviting outside legal, technical, or data governance experts to provide legitimacy and help explain complex topics. Provide written materials describing privacy safeguards, the presentation, and provide additional detail.

AGENDA ITEM	RECOMMENDED LENGTH	NOTES
Break/Transition time	10 minutes	If the meeting will last more than 90 minutes, include a break.
Engagement Activity Examples: › Ask stakeholders to review potential use cases or research questions, add new ones, and rank their priorities with stickers. › Solicit stakeholders' insight and lived experiences about their administrative records and your potential use case, to reveal factors and nuance that may not be captured by the data. › Interview stakeholders about their privacy norms and preferences (e.g., are they comfortable with A data point(s) being used by B organization(s) for C purpose, with XYZ controls or conditions in place?)	30–60 minutes	Led by a core IDS planning team member with strong facilitation skills. For early-stage IDS, engagement activities are especially effective for agenda-setting and vetting data governance policies. Depending on the number of participants, consider using more hands-on and small group activities for engagements 45 minutes or longer. See the *Convening Stakeholders Worksheet* in Appendix C.4 for more considerations in crafting an engagement activity.
Closing and Next Steps	5-10 minutes	Identify next steps, upcoming opportunities for engagement, and who stakeholders should contact to learn more.

C.9: Sample — Interagency IDS Retreat Agenda

An interagency retreat can be helpful in establishing shared expectations for your IDS, building agency buy-in, and prioritizing your IDS research agenda. You may find a retreat useful at the beginning of your IDS process, or as a strategy for refocusing or reinvigorating your IDS as it evolves. The meeting agenda template below can be customized to fit your local context and stage of development but should always include some level-setting up front about the scope of your integration effort and how individual privacy will be protected.

Recommended meeting length: 2-3 hours

Recommended attendees: agency leaders and staff involved in research, evaluation, and policy analysis

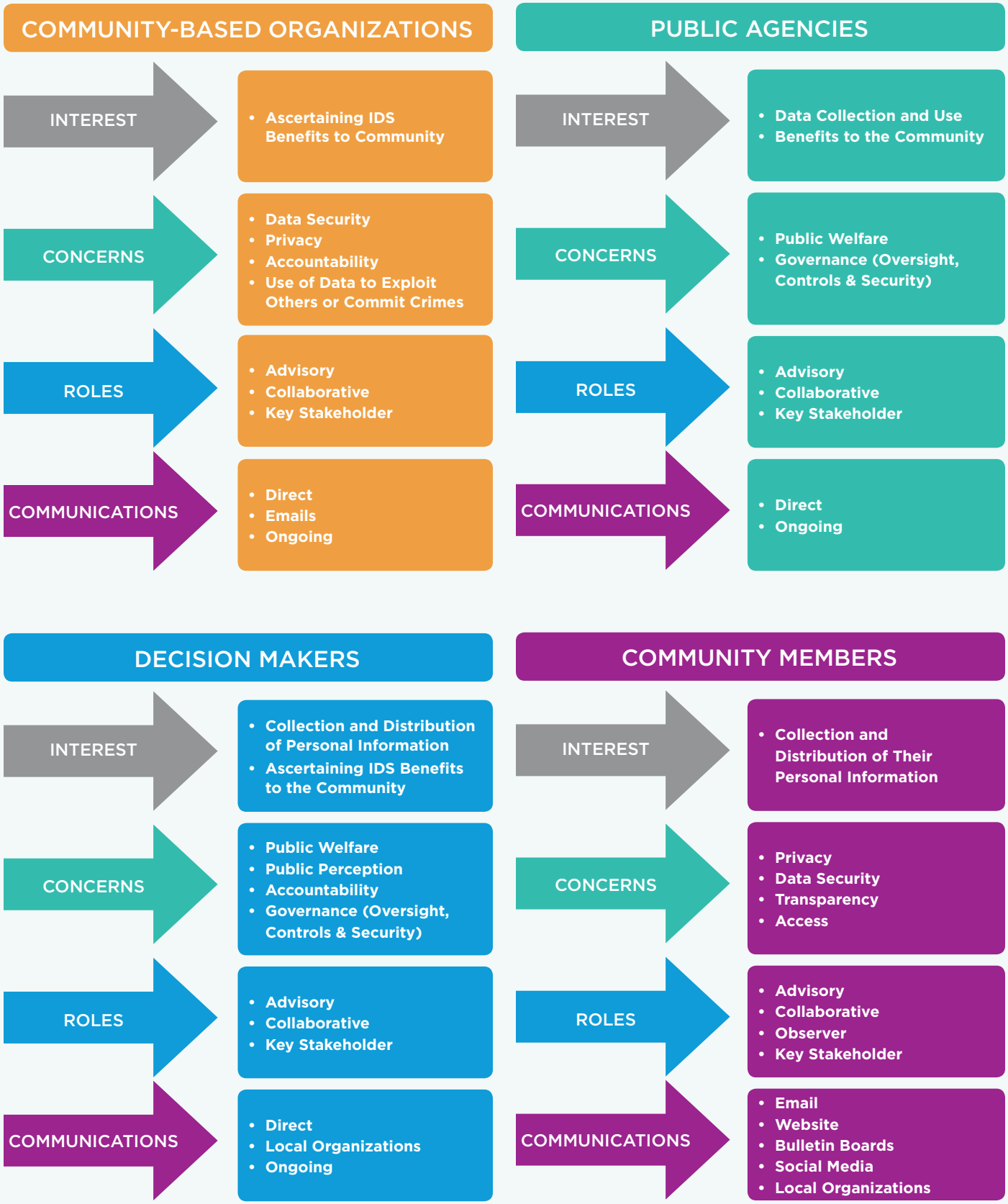
Questions to ask yourself when planning a retreat:

- What agencies have already expressed interest in integrating data?
- What agencies hold high-value data but have not yet been engaged?
- What decisions have already been made?
- What decisions need to be made?
- How can agency leaders and staff be most helpful in informing those decisions?

INTERAGENCY RETREAT SAMPLE AGENDA

AGENDA ITEM	RECOMMENDED LENGTH	NOTES
Registration & Breakfast or Lunch	30 minutes	
Welcome & Introductions Who are we? Why are we here today?	5–10 minutes	Led by a core IDS planning team member with strong communications skills.
Opening Remarks Why is this IDS a priority? What do we hope to achieve?	5–10 minutes	Can be as formal or informal as you like but should feel like a cheerleading moment and be led by a high-level champion of the work (policy-makers, agency head, etc.).
Framing the Effort Who else is doing this work? What lessons can we learn from them? Why is it important that it's done with strong community engagement?	10–15 minutes	This is often best led by an outside expert or guest from a neighboring IDS.
Level-Setting Where are we in the IDS development process? What is this IDS and what is it not? How will data uses be approved and by whom? How will individual privacy be protected?	15–30 minutes	Led by a core IDS planning team member with strong communications skills.
Break	10 minutes	
Small Group Discussion — Within Agency What are your agency's highest priority policy, research, and evaluation questions? Which of these questions requires data from other agencies to be answered meaningfully? Which datasets or data points would you need and who collects them?	30–45 minutes	This is designed to surface the "what's in it for me" of data sharing for each agency and create an initial list of potential high-priority IDS use cases. Use chart paper to record the brainstorm at each table.
Break/Transition Time	10 minutes	
Small Group Discussion — Interagency	15–30 minutes	Rotate seating so that each table includes representatives from several agencies and then repeat the first exercise.
Gallery Walk or Dot Voting Which of the questions that have been brainstormed are highest priority, which are most doable, which are most fundable, etc.?	10–15 minutes	This is a time to allow all participants to browse the brainstorms created by other tables. You may also ask participants to vote for their highest priority use cases using stickers or simply initials.
Closing & Next Steps	5–10 minutes	

C.10: Sample — IDS Stakeholder Analysis



APPENDIX D: ADDITIONAL RESOURCES

Although the following list of resources is presented with general topics for ease of use, there is some overlap in subject matter.

Administrative and Integrated Data Backgrounders

- Administrative Data Research Facilities (ADRF) Network Working Group, *Communicating about Data Privacy and Security* (2018), https://docs.wixstatic.com/ugd/e35e20_411ab2738ba54873b2995c7389ee489b.pdf.
- Centre for Public Impact (BCG), *A Brief Introduction to…Evidence-Informed Policymaking* (June 2018), https://resources.centreforpublicimpact.org/production/2018/07/No-2-CPI-A-brief-introduction-to...Evidence-informed-policymaking-FINAL-sm..pdf.
- Commission on Evidence-Based Policymaking, The Promise of Evidence-Based Policymaking (Sept. 2017), https://www.cep.gov/content/dam/cep/report/cep-final-report.pdf.
- Linda Gibbs et al., *IDS Governance: Setting Up for Ethical and Effective Use, AISP Expert Panel Report* (2017), https://www.aisp.upenn.edu/wp-content/uploads/2016/07/Governance.pdf.
- Powered by Data, *Maximizing Impact through Administrative Data Sharing: Transform the Sector* (2018), https://static1.squarespace.com/static/5623f0e8e4b012625405337/t/5aea197d0e2e7278ee175dc9/1525291389930/GENERAL+-+Transform+the+Sector+Briefing+Doc.pdf.
- State Data Sharing Initiative, *Data Sharing Toolkit* (2018), http://www.statedatasharing.org/data-sharing/#toolkit.

Stakeholder Communications and Engagement Tools

- 18F, *18F Method Cards: A Collection of Tools to Bring Human-Centered Design into your Project*, https://methods.18f.gov/.
- BSR, *Back to Basics: How to Make Stakeholder Engagement Meaningful for Your Company* (2012), https://www.bsr.org/reports/BSR_Five-Step_Guide_to_Stakeholder_Engagement.pdf.
- Cabinet Office (UK), *Open Policy Making toolkit: Sensitive Policy Tools* (Jan. 2017), https://www.gov.uk/guidance/open-policy-making-toolkit/sensitive-policy-tools.
- Civic Tech & Data Collaborative (CTDC), *The CTDC Toolkit: Ingredients of a Civic Tech and Data Collaborative* (2018), https://medium.com/civic-tech-data-collaborative/the-ctdc-toolkit-ingredients-of-a-civic-tech-and-data-collaborative-beb2d59858c6.
- Department for Digital, Culture, Media & Sport (UK), *Data Ethics Workbook* (June 13, 2018), https://www.gov.uk/government/publications/data-ethics-workbook/data-ethics-workbook.
- Digital.Govt.NZ (New Zealand), *How to Develop an Online Engagement Strategy* (June 20, 2018), https://webtoolkit.govt.nz/guidance/online-engagement/engagement-strategy-template/.
- Environmental Protection Agency, *Public Participation Guide* https://www.epa.gov/international-cooperation/public-participation-guide.
- Francis Gouillart and Tina Hallet, *Co-Creation in Government*, Stanford Social Innovation Review (2015), https://ssir.org/articles/entry/co_creation_in_government.
- GovExLabs, *Guides*, https://labs.centerforgov.org/guides/.
- GovLab, *People-Led Innovation: Toward a Methodology for Solving Urban Problems in the 21st Century* (2018), http://www.thegovlab.org/static/files/publications/people-led.pdf.
- Human Resources and Skills Development Canada, *Guide to Planning Inclusive Meetings* (2009), http://publications.gc.ca/collections/collection_2010/rhdcc-hrsdc/HS28-141-2009-eng.pdf.
- Information Commissioner's Office (UK), *Think Privacy Toolkit For Organizations*, https://ico.org.uk/media/for-organisations/think-privacy/2693/ico-think-privacy-toolkit.pdf.
- Institute for Local Government, *Preparing for Successful Public Meetings: Checklist for Before, During, and After* (Oct. 2013), https://www.ca-ilg.org/sites/main/files/file-attachments/meeting_preparation_checklist_.pdf.
- Lane et al., *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (2014).

- National Oceanic and Atmospheric Administration, *Introduction to Planning and Facilitating Effective Meetings* (2010), https://coast.noaa.gov/data/digitalcoast/pdf/effective-meetings.pdf.
- NYC Mayor's Office for the Economic Opportunity, *NYC Civic Service Design Tools + Tactics* (2017), https://www1.nyc.gov/assets/servicedesign/index.html.
- Open Government Partnership, *OGP's Participation and Co-Creation Toolkit: From Usual Suspects to Business as Usual* (May 2018), https://www.opengovpartnership.org/stories/ogps-participation-and-co-creation-toolkit-usual-suspects-business-usual.
- Torfaen County Borough Council, *Stakeholder Engagement – A Toolkit: Working Towards More Effective and Sustainable Brownfield Revitalisation Policies* (2007), https://www.envpmsolutions.ca/images/27_stakeholder_engagement_a_toolkit-2.pdf.

Domain-Specific Guidance

Child welfare:

- Western and Pacific Child Welfare Implementation Center, *Stakeholder Engagement Tools for Action* (2013), https://www.cssp.org/publications/general/WPIC_DCFS_Stakeholder_Engagement_Toolkit.pdf.

Diverse and under-represented communities:

- City of Seattle Office for Civil Rights, *Inclusive Outreach And Public Engagement Guide* (Apr. 2009), https://www.seattle.gov/Documents/Departments/ParksAndRecreation/Business/RFPs/Attachment5%20_InclusiveOutreachandPublicEngagement.pdf.
- Michael Lenczner, *First Nations Data Sovereignty and the OCAP® Principles*, Knowledge Centre (Aug. 1, 2018), https://share.otf.ca/t/first-nations-data-sovereignty-and-the-ocap-principles/793.
- University of Washington, *Diverse Voices: A How-to Guide for Facilitating Inclusiveness In Tech Policy* (Aug. 2017), http://techpolicylab.org/wp-content/uploads/2017/08/TPL_Diverse_Voices_How-To_Guide_2017.pdf.

Education:

- Susan N. Bales, *Framing Education Reform*, FrameWorks Institute (Jan. 2010) http://www.frameworksinstitute.org/assets/files/PDF_Education/education_message_memo.pdf.
- Data Quality Campaign (DQC), *More Than a Number: Tools for Talking about Education Data* (2017), https://dataqualitycampaign.org/CommsToolkit/.
- ExcelinEd, *Student Data Privacy Communications Toolkit* (Apr. 2016), https://www.excelined.org/wp-content/uploads/Student-Data-Privacy-Comms-Toolkit.pdf.
- Privacy Technical Assistance Center (PTAC), U.S. Department of Education, *Data Governance Checklist* (June 2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Governance%20Checklist_0.pdf.
- PTAC, *Integrated Data Systems and Student Privacy* (Jan. 2017), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/IDS-Final.pdf.

Health care:

- Involve, the Carnegie UK Trust, and Understanding Patient Data, *Data for Public Benefit: Balancing the Risks and Benefits of Data Sharing* (2018), https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2018/04/Data-for-Public-Benefit-REPORT.pdf.
- National Center for Health Statistics, *Toolkit for Communities Using Health Data* (May 2015) https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/Toolkit-for-Communities.pdf.
- Understanding Patient Data, *Supporting Conversations Resources*, https://understandingpatientdata.org.uk/supporting-conversations.

Neighborhood information:

- National Neighborhood Indicators Partnership (NNIP), *NNIP's Resource Guide to Data Governance and Security* (Sept. 2018), https://www.urban.org/sites/default/files/publication/98997/nnips_resource_guide_to_data_governance_and_security_0.pdf.

ENDNOTES

1 Joel Gehman et al., Social License to Operate: Legitimacy by Another Name?, 60 Can Pub Admin 293 (2017), https://onlinelibrary.wiley.com/doi/full/10.1111/capa.12218.

2 *A Brief Introduction to... Evidence-Informed Policymaking*, Ctr Pub Impact (Jun. 2018), https://resources.centreforpublicimpact.org/production/2018/07/No-2-CPI-A-brief-introduction-to...Evidence-informed-policymaking-FINAL-sm..pdf; The Skeptic's Guide to Open Government, Open Gov Partnership (Jul. 2018), https://www.opengovpartnership.org/sites/default/files/SKEPTICS-GUIDE_20180710.pdf.

3 *Maximizing Impact through Administrative Data Sharing: Transform the Sector, Powered By Data* (Jun. 2018), https://static1.squarespace.com/static/5623f0e8e4b0126254053337/t/5aea197d0e2e7278ee175dc9/1525291389930/GENERAL+-+Transform+the+Sector+Briefing+Doc.pdf https://static1.squarespace.com/static/5623f0e8e4b0126254053337/t/5aea197d0e2e7278ee175dc9/1525291389930/GENERAL+-+Transform+the+Sector+Briefing+Doc.pdf; *Major Takeaways from the Governor's Vetoes*, SCPC (Jul. 12, 2018), https://www.scpolicycouncil.org/featured/major-takeaways-from-the-governors-vetoes.

4 Pam Carter et al., *The Social Licence for Research: Why care.data Ran into Trouble*, 41 J Med Ethics 404 (2015), https://jme.bmj.com/content/41/5/404.

5 Douglas MacKay & Averi Chakrabarti, *Government Policy Experiments and Informed Consent, Pub Health Ethics* (Aug. 2018), https://academic.oup.com/phe/advance-article-abstract/doi/10.1093/phe/phy015/5063429?redirectedFrom=fulltext; Kaela Scott et al., Data for Public Benefit: Balancing the Risks and Benefits of Data Sharing, CarnegieUK Trust (Apr. 2018), https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2018/04/Data-for-Public-Benefit-REPORT.pdf

6 IAP2 Public Participation Spectrum, IAP2, https://www2.fgcu.edu/Provost/files/IAP_Public_Participation_Spectrum.pdf.

7 Andrew Young et al., People-Led Innovation: Toward a Methodology for Solving Urban Problems in the 21st Century, GovLab (Jan. 2018), http://www.thegovlab.org/people-led-innovation.

8 Adapted from Jonathan Morris & Farid Baddache, Back to Basics: How to Make Stakeholder Engagement Meaningful for Your Company, BSR (Jan. 2012), https://www.bsr.org/reports/BSR_Five-Step_Guide_to_Stakeholder_Engagement.pdf.

9 Morris, supra note 9.

10 Article 12 of Universal Declaration of Human Rights states: "No one must be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation." Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948). In his dissent in Olmstead v. United States, Justice Brandeis noted that "the right to be let alone [is] the most comprehensive of rights and the right most valued by civilized men." Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

11 There may be significant cultural variation in how individuals weigh privacy interests against other values, such as community cohesion or public safety.

12 Sean Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST (2017), https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

13 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 511, 530 (2006); *Consent, Data-Driven Inequities, and The Risks of Sharing Administrative Data*, Powered by Data (June 25, 2018), https://poweredbydata.org/blog/2018/6/25/risks-of-sharing-administrative-data.

14 Abigail Geiger, *How Americans have Viewed Government Surveillance and Privacy Since Snowden Leaks*, Pew Research Ctr (Sept. 14, 2018), http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/; Chris Kahn & David Ingram, *Americans Less Likely to Trust Facebook than Rivals on Personal Data*, Reuters (Mar. 25, 2018, 8:04 AM), https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3.

15 Scott Shane & Daisuke Wakabayashi, *The Business of War: Google Employees Protest Work for Pentagon*, NY Times (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.

16 Valerie Strauss, *$100 Million Gates-Funded Student Data Project Ends in Failure*, Wash. Post (Apr. 21, 2014), https://www.washingtonpost.com/news/answer-sheet/wp/2014/04/21/100-million-gates-funded-student-data-project-ends-in-failure/.

17 Monica Bulger et al., *The Legacy of inBloom*, Data & Society (Feb. 2, 2017), https://datasociety.net/output/the-legacy-of-inbloom/.

18 *Research Ethics in the Data Sciences*, Wash U, https://courses.washington.edu/bethics/violations.html; *Research & Economic Development: Office of the Vice Chancellor*, UMKC, http://ors.umkc.edu/research-compliance-(iacuc-ibc-irb-rsc)/institutional-review-board-(irb)/history-of-research-ethics/irb-historical-incidents-related-to-human-subjects-protections; Khaliah Barnes, *Agencies Behaving Badly: Government Surveillance and Privacy Act Violations*, Jurist (Jan. 2, 2014, 12:00 PM), http://www.jurist.org/hotline/2014/01/khaliah-barnes-privacy-act.php.

19 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (2018).

20 *E.g.*, Tonyaa Wathersbee, *Donald Trump Immigration Policy Puts Rural America in Danger*, USA Today (Aug. 2, 2018, 6:59 PM), https://www.usatoday.com/story/opinion/policing/data-casualties/2018/08/02/crime-immigration-ice-donald-trump-policing-usa/883946002/.

21 What is and is not considered sensitive varies depending on legal, technical, and cultural factors. See, *Sensitive Data Chart*, https://www.teachprivacy.com/wp-content/uploads/Sensitive-Data-Chart-by-K-Royal-01.xlsx.

22 Over time, as technologies and the global privacy context have changed, the FIPPs have been presented in different ways with different emphases. For a full history of the changes that have been made to the FIPPs, see Robert Gellman, *Fair Information Practices: A Basic History* (Apr. 10, 2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

23 Ehren Helmut Pflugfelder, *Reddit's "Explain Like I'm Five": Technical Descriptions in the Wild*, 26 Tech Comm Q 25 (2017), https://www.tandfonline.com/doi/abs/10.1080/10572252.2016.1257741?journalCode=htcq20.

24 *Rubber Duck Debugging*, https://rubberduckdebugging.com/.

25 *The Up-Goer Five Text Editor*, http://splasho.com/upgoer5 (an instrument that challenges people to explain hard concepts using only the 10,000 most common English words).

26 *Sideways Dictionary*, https://sidewaysdictionary.com/#/ (alternative definitions of technical terms).

27 *Connected Health Cities*, https://www.connectedhealthcities.org/get-involved/glossary-data-use/#content.

28 *Intro to IDS, Actionable Intelligence for Social Policy (AISP),* https://www.aisp.upenn.edu/integrated-data-systems/what-is-an-ids/.

29 E.g., Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, NYU Pub L & Leg Theory Working Papers (2010), https://lsr.nellco.org/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1534&context=nyu_plltwp; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L Rev 1701 (2010), https://www.uclalawreview.org/pdf/57-6-3.pdf; Jules Polonetsky et al., *Shades of Gray: Seeing the Full Spectrum of Practical Data De-Identification*, 56 Santa Clara L Rev 593 (2016), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2827&context=lawreview.

30 Kelsey Finch, *A Visual Guide to Practical Data De-Identification*, FPF (Apr. 25, 2016), https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/; Simson L. Garfinkel, De- Identification of Personal Information, NIST (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf

31 Adapted from *Working Towards More Effective and Sustainable Brownfield Revitalization Policies*, REVIT (2007), https://www.envpmsolutions.ca/images/27_stakeholder_engagement_a_toolkit-2.pdf.

32 Adapted from *Plan Your Online Engagement*, Digital.Govt.NZ (last updated Jun. 20, 2018), https://webtoolkit.govt.nz/guidance/online-engagement/engagement-strategy-template/

33 *Id*.

34 Chatham House, *Chatham House Rule*, https://www.chathamhouse.org/chatham-house-rule.

35 Adapted from REVIT, *supra* note 35.

36 Linda Gibbs et al., *IDS Governance: Setting Up for Ethical and Effective Use, AISP Expert Panel Report* (2017), https://www.aisp.upenn.edu/wp-content/uploads/2016/07/Governance.pdf.

37 Adapted from Magassa, *supra* note 11.

38 See Chatham House, *supra* note 36.

39 *All Are Welcome: Hosting People with Disabilities*, Chromis Events (Sept. 14, 2017), https://www.chromisevents.com/all-are-welcome-hosting-people-with-disabilities/.

40 City of Seattle Office for Civil Rights, *Inclusive Outreach And Public Engagement Guide* (Apr. 2009), https://www.seattle.gov/Documents/Departments/ParksAndRecreation/Business/RFPs/Attachment5%20_InclusiveOutreachandPublicEngagement.pdf.

41 University of Washington, *Diverse Voices: A How-to Guide for Facilitating Inclusiveness In Tech Policy* (Aug. 2017), http://techpolicylab.org/wp-content/uploads/2017/08/TPL_Diverse_Voices_How-To_Guide_2017.pdf.

42 Kelsey Finch et al., *Communicating about Data Privacy and Security*, Admin Data Research Facilities Network (Jun. 2018), https://docs.wixstatic.com/ugd/e35e20_411ab2738ba54873b2995c7389ee489b.pdf.

43 See Chatham House, *supra* note 36.

About FPF: Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

About AISP: Established at the University of Pennsylvania in 2008, Actionable Intelligence for Social Policy (AISP) works with state and local governments to develop Integrated Data Systems (IDS) that link administrative data across government agencies. IDS give governments and their partners the ability to better understand the needs of individuals and communities and improve programs and practices through evidence-based collaboration.

FUTURE OF PRIVACY FORUM

ACTIONABLE INTELLIGENCE FOR SOCIAL POLICY

1400 Eye Street NW | Suite 450 | Washington, DC 20005 | FPF.org