Privacy Risk Assessment for Smart & Connected Communities

When responsible organizations identify new ways to process data, for example, when launching a new program, product, system or service, they utilize Privacy Impact Assessments (PIA) or risk assessments to conduct a systematic analysis to identify and address privacy issues. Current PIA practice includes detailed frameworks to help privacy professionals understand and quantify privacy risks. Yet accounting for risks is only part of a balanced value equation. Decision-makers must also assess, prioritize, and to the extent possible, quantify a project's benefits in order to understand whether assuming the risk is appropriate.

Local governments in particular are stewards to the data of highly diverse stakeholders, and must account for privacy priorities and sensitivities that may vary widely among their constituent communities. A thorough assessment of privacy risks should take into account considerations beyond data protection and security, including ethics, equity, and public engagement.

For our workshop

Who is this for? Smart and connected community leaders and their technology/service providers and partners.

What does this do? Help communities and their partners identify the full array of data-related risks around emerging technologies and data flows, so that they can be appropriately managed and mitigated.

What's in scope for 'smart communities'? Any product or service that uses personal data and/or connected technologies to provide a public good. (Examples include: connectivity/broadband initiatives, infrastructure sensors, sensitive data analytics, transportation initiatives, civic identity systems; open data programs; integrated data systems, policy evaluation, and performance management; etc.)

What's unique or interesting about smart communities and privacy risks?

- Public-private partnership and vendor management complications
- Open data commitments and public record requirements
- Equity is not an option, it's a requirement
- Your data or your life: opting out of public services
- Conflicts between important public values and diverse stakeholder groups
- Public and private spaces, and their expectations of privacy, are blurring
- Power asymmetries between government and individuals

Caveats:

- This is an early draft! Much of the language still needs to be smoothed out, lists and exemplars need to be fleshed out, and scoping needs to continue.
- Many of the determinations to be made are inherently subjective. What's important is proactively thinking through the questions and issues, considering appropriate steps to address risks, and being able to explain your decisions before collecting or using personal data.
- Communities should adapt this framework to fit their own needs, resources, and public priorities.

Questions for reviewers:

- What is the most helpful piece we can bring to the PIA process:
  - Structured options for identifying particular risk factors as higher or lower than others?
  - Substantive case studies around particular "smart city"/emerging technologies or data uses?
  - Highlighting guidance and educational resources, or explaining the relevance of particular questions?
  - Catalogues of common privacy harms/adverse actions and/or controls and safeguards?
- What else is important here? What have your experiences or key learnings been around data risks in smart community projects?

Comments and suggestions welcomed: kfinch@fpf.org

I. Putting Personal Data and Projects into Context

a. Describe the project:

i. What is the purpose of collecting an dusing personal data within this project? What outcomes do you want to achieve? How does this project advance your organization's public mission?
ii. Who do you expect to benefit from this project's collection and use of personal data (e.g., society at large, specific neighborhoods, an agency or institution, particular individuals or constituents, etc.)? What *direct* benefits will individuals and local communities see from this project?
iii. What are the functional capabilities needed to carry out this project?
iv. Who is involved in this project, and what are their roles? Please include internal and external staff, partners, service providers, advisors, users, etc. (E.g. Who hosts the data and services? Who communicates with the public and other stakeholders? Who maintains and secures the system? Who analyzes the data? Who oversees the project team? Who manages privacy safeguards and controls?)
v. What is the estimated project timeline, and how will personal data be handled when/if the project is wound up or dissolved? (E.g. Is this a pilot or a long-term project? Are there any relevant retention schedules or obligations for this data?)
vi. Is this project the least burdensome alternative with respect to data privacy? Could this project be conducted in ways that accomplish the same goal while minimizing the impacts on individual privacy? Could this project be altered to enhance privacy protections?
vii. Describe any other relevant details about the project's organization and goals.

b. Describe the project's legal environment:

i. Describe any specific laws, standards, or other commitments that this project must operate within (e.g., state, local, or federal laws; public records acts; your organization's privacy policy; security standards; a code of conduct; privacy by design principles; ethical or social justice obligations; community engagement commitments; contractual requirements; privacy-preserving features that you plan to highlight or market to users, etc.?)
ii. How mature is the legal framework that addresses this project's collection and use of personal data? (E.g., Is there a significant body of relevant case law or best practices? Has this framework recently been challenged or revised? Have other organizations conducted similar projects? Are there experts in this field that could be consulted?)
iii. What is your organization's risk tolerance for data privacy?
iv. Are project staff, sponsors, and partners familiar with data processing and privacy protections in this field? (E.g., Do project staff have privacy training? Are vendor contracts tailored for this project or your organization, rather than commercial boilerplate? Are public sponsors of the project able to speak to privacy issues? Have any experts been consulted?)
v. Is any of the personal data used for this project already being collected by other means or used for other purposes? If so, describe how it is used and protected in those contexts.

c. Describe the project's social environment:

i. Has the project been announced publicly? If so, describe how and by which organizations.
ii. Are any other municipalities/counties conducting substantially similar projects? If so, describe how they have addressed privacy concerns.
iii. How active are privacy discussions in your community and your project area? (E.g., Is there a dedicated privacy advisory commission? Are there dedicated advocacy or community groups? Is this a frequently studied technology or service, or something brand new? Have any impacted communities experienced privacy violations in the past?)
iv. Describe the public perception or posture of participating organizations regarding data privacy. Is there existing "privacy baggage" from any party to this project[1]? (E.g., high expectations of privacy from a healthcare institution or public agency, low expectations of privacy or mistrust for a technology partner or funder with a checkered reputation on privacy, an agency or institution with a history of ethical violations, an advocacy group focused on privacy or data equity, etc.)
v. Will this project's collection and use of personal data be validated or legitimized by civic leaders or democratic bodies, as appropriate? (E.g., public hearings, debates, legislative processes, executive orders, community engagement, etc.)

[1] *Note: Privacy "baggage" of this sort is not necessarily disqualifying, but indicates that additional steps should be taken to earn public trust in this project.*

d. **Describe the personal data that is part of this project[2]:**
   i. What data elements in this project could directly or indirectly (whether alone or in combination) identify an individual person? (E.g., contact information, account information, demographic information, device identifiers, and some precise geolocation information)
   ii. What data elements in this project could single out an individual or group, even if they could not identify any particular person?
   iii. What data elements in this project are considered de-identified or anonymous? Describe any technical, legal, and organizational safeguards designed to reduce the risk of re-identification.
   iv. What data elements in this project could be considered sensitive or otherwise highly personal personal information? (E.g., location data, children's data, data about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation)
   v. What data elements in this project are considered confidential for non-privacy reasons? (E.g., critical infrastructure, public safety information, IP, etc.)
   vi. What data elements in this project will be collected in unstructured or unusual formats? (E.g., video/audio, free text fields, biometric/genetic information, AI or algorithmically-generated data?)

e. **Describe the collection process:**
   i. What is the legitimate basis for obtaining personal information for this project? (E.g., the collection is authorized by law or public policy, individual consent, there is social license to collect and use personal information for these purposes, this data is necessary to protect the rights and interests of individuals or groups, etc.)
   ii. Is personal data being collected primarily for the purpose of this project, or was it originally collected for another, different purpose? If this is a secondary use, describe the purposes for which the data was originally collected and explain why they are or are not compatible with this secondary use. (E.g., internal product development, security, fraud detection, research, monetization, etc.)
   iii. How is personal data for this project going to be obtained?
      1. Directly from individual for this purpose (e.g., surveys, administrative records, solicited comments, etc.)
      2. Observed or inferred (e.g., sensors, utilities usage, public video/audio, metadata, etc.)
      3. From another government agency (either intra- or inter-governmental)
      4. From a nonprofit data provider (e.g., academic institution, NGO, community organization, etc.)
      5. From a commercial data provider (e.g., analytics provider, social media, website provider, data broker, etc.)
      6. Other
      7. Don't know
   iv. Will new data be derived or aggregated from the personal data obtained for this project? If so, which data elements will be used to do so?
   v. If personal data is obtained from a third party, describe the due diligence conducted before acquiring it. (E.g., Does the third party have a legitimate basis to collect and share the data with you, for this purpose? Is this organization trustworthy? Would individuals be surprised that their data has been shared with you?)
   vi. Is there anything potentially controversial about how the personal data for this project was collected? (E.g., was the data collected through surveillance equipment, was it collected in a public or private space, was it collected for another purpose, would individuals have had a reasonable expectation of privacy in that context?)

II. Fundamental Principles of Personal Data

a. **Describe the flow of personal data in this project:**
   i. Describe in detail the full lifecycle of personal data in this project, including each step at which personal data is transferred, analyzed, combined, stored, destroyed, or otherwise processed.

b. **Describe how personal data will be adequate, relevant, and limited to what is necessary for this project:**

[2] *Tip: Consider applicable federal, state, and local laws and guidance in answering these questions, and err on the side of caution. There can be significant legal and cultural variability about how data is categorized.*

i. What is the minimum viable personal data required for this project?
ii. What is/are the specific purpose(s) for each type of personal data to be collected or used in this project (including data that is derived, aggregated, or de-identified)? Describe how the personal data is necessary and proportionate to the purpose and goals of the project, as narrowly and concretely as possible.
iii. In what ways will the collection of unnecessary personal data be minimized? (E.g., Avoiding free text fields or providing warnings to users not to share personal information; avoiding the incidental collection of metadata; limiting the scale or scope of sensing devices; immediate de-identification or deletion of certain fields; etc.)
iv. If physical devices are deployed as part of this project, will they have built-in hardware or software options to limit the collection of personal data (E.g., deactivated features, mute buttons, software toggles, manual activation for data collection, etc.)?

c. **Describe how personal data will be retained or stored during this project:**
i. How long is it necessary to retain personal data for this project in identifiable form? If personal data will be stored for any longer than necessary to accomplish the purposes for which it was collected, describe why. (E.g., compliance with record retention requirements, peer review or evaluation requirements, for security purposes, etc.)
ii. How long will de-identified data for this project be retained?

d. **Describe how data quality will be maintained for this project:**
i. How will personal data for this project be kept accurate, complete, and current? (E.g., specific policies or procedures, staff training, routine reviews, automated checks or audits, etc.)
ii. What will occur if personal data is found to be inaccurate or outdated? (E.g., automatic correction, notification of impacted individuals,
iii. Are there mechanisms for individuals to submit corrections to potentially inaccurate personal data?
iv. Will changes to personal data be logged or traced in some way? If so, how?
v. If de-identification or security procedures introduce noise or otherwise compromise the accuracy of the personal data used for this project, will that introduce significant inaccuracies or biases? If so, how will that risk be mitigated?

e. **Describe how personal data will be appropriately deleted or de-identified for this project:**
i. In what circumstances will personal data be deleted, destroyed, or de-identified?
ii. How will personal data (including backups) be deleted or destroyed when appropriate for this project? (E.g., securely overwriting files, file shredding, purchased software or vendor support, etc.)
iii. How will personal data be de-identified when appropriate for this project? (E.g., differentially private solutions, statistical disclosure controls, in-house solution, purchased software, trusted third party, expert analysis, etc.)
iv. How often will re-identification risk be assessed?

f. **Describe how personal data will be appropriately secured for this project:**
i. Does your organization maintain a comprehensive written data security plan and reasonable data security practices to protect the confidentiality, integrity, and availability of personal data?
ii. Describe the reasonable technical, physical, and administrative safeguards that will protect this project's personal data from unauthorized use or disclosure. (E.g., vulnerability assessments, encryption, access controls, password protocols, data partitions, etc.).
iii. If this project is subject to a data breach, which entity(ies) are responsible for responding to the incident and alerting the public and any relevant authorities? How will they do so?
iv. Is there an organizational plan for receiving, reviewing, and addressing security vulnerability reports from third parties, including researchers, academics, or other members of the public?
v. Will personal data be encrypted in transit and/or at rest at any point during this project lifecycle? If so, describe when and the encryptions standard to be used.

III. Transparency and Public Engagement

a. **Describe how notice about the collection and use of personal data will be provided:**

i. Will there be a clear and conspicuous, publicly available privacy policy or other online privacy documentation for this project? If so, describe where and how it will be made available. Such a policy should specifically describe:
    1. How personal data is collected, used, shared, stored, disposed of, and secured;
    2. Whether any information will or could be made public (such as through an open data program or public records requests);
    3. Any de-identification commitments or techniques in use;
    4. How individuals can exercise any choices or rights available to them, including any opt-outs and ability to access, correct, or delete data about themselves;
    5. Whether personal data will be used for advertising, for research, for other specified purposes;
    6. Under what conditions will personal data be made available to law enforcement or other government agencies;
    7. Any data sharing agreements or other partnerships where their personal data might be jointly held;
    8. Whether automated decision-making or profiling occurs, and if so the logic involved and significance and envisaged consequences for individuals.
ii. Describe how your project will be marketed, with respect to any privacy-preserving functionality.
iii. Will individuals be notified about this project's use of personal data before or at the time their data is collected? If so, how[3]? If not, what is the justification for not providing advanced notice? If not, will individuals be informed about the collection and use of their personal data within a reasonable time afterwards?
iv. If new data collection capabilities are added or if personal data is used in a new way in the course of this project, will individuals be notified beforehand? If so, how? If not, what is the justification for not providing advanced notice? If not, will individuals be informed about the collection and use of their personal data within a reasonable time afterwards?
v. If data will be collected indirectly (i.e. personal data obtained through observation, inference, or provided by a third party), will individuals be informed about how the data was obtained and from what source? If so, how? If not, what is the justification for not providing this information? (E.g., contractual or confidentiality obligations, exemption from public records acts, etc.)
vi. Will individuals be notified before their personal information is shared with a third party? If so, how? If not, what is the justification for not providing advanced notice? If not, will individuals be informed about the sharing of their personal data within a reasonable time afterwards?
vii. If and when the project is ended, will individuals be notified and informed about how their personal data will be handled during and after the dissolution?
viii. Will accessible notice mechanisms be developed for persons with disabilities, persons with limited English proficiency, or other vulnerable or marginalized individuals?

b. Describe how this project will meaningfully communicate and inclusively engage with stakeholders and the public around data and privacy:

i. Describe any community engagement strategies specific to this project's collection and use of personal data, and how it is inclusive of diverse stakeholders. (E.g., town halls, public notice and comment periods, tech fairs, community meetings, unconferences, advisory panels, public ballots, crowdsourcing platforms, etc.)
ii. Describe when and in what ways this project will solicit and incorporate public and stakeholder input and feedback on data privacy throughout the project lifecycle.
iii. Have all relevant stakeholders[4] in this project, including impacted individuals or their representatives, been given a chance to express their views on the proposed collection and use of individuals' data? Describe those views.

[3] E.g., online privacy policy, lights or noises on connected devices, just-in-time permissions or push notifications on associated apps, community education and awareness campaigns, public signage or iconography, individual data dashboards, complaint lines, etc.

[4] Consider both internal stakeholders (e.g., sponsors, funders, oversight bodies, partners, service providers, etc.) and external stakeholders (e.g., community groups, impacted individuals, media outlets, advocacy organizations, industry organizations, governmental bodies, academic institutions, or others).

iv. Describe any existing relationships between individuals or groups whose personal data will be collected and used in this project and your organization or its partners Describe the degree of information technology experience/understanding by individuals and groups impacted by this project's collection and use of personal data. Will this project necessitate data literacy support for local communities or other stakeholders?
v. If a physical device will be deployed as part of this project, has the local community been given an opportunity to request or reject its placement?

IV. Choices and Individual Rights

a. Describe the role of individual consent in this project:

i. Is an individual's explicit consent obtained prior to the collection or use of their personal data? If so, how? If not, is explicit consent obtained at some other point in time?
ii. Is an individual's implicit consent relied upon for the collection or use of personal data as part of this project? If so, describe for which purposes and how that consent will be expressed.
iii. If individuals are provided granular choices about how their personal data will be collected and used and shared for this project, when and how can they exercise them? (E.g., centralized opt-ins/outs for certain uses of data, a dashboard of controls for sharing fully versus partially identified data for certain purposes, app permissions or platform settings to reset identifiers, do not track signals, pseudonymous or anonymous guest accounts, etc.)
iv. Will individuals be prompted to renew their consent at any point in time? Are individuals able to alter or withdraw consent they previously provided? If so, describe how and what the impacts of withdrawing consent would be.
v. Are the individual's choices and changes to those choices communicated to third parties to whom their information has been disclosed? If so, how? If not, why not?
vi. Will accessible consent mechanisms be developed for persons with disabilities, persons with limited English proficiency, or other vulnerable or marginalized individuals?

b. Describe consent for sensitive data and vulnerable persons:

i. Is an individual's explicit consent obtained prior to collecting or using their sensitive personal information for this project? (e.g., location information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and genetic data or data concerning health or sex life and sexual orientation, etc.).
ii. If children's personal data is collected or used for this project, will explicit be consent obtained from their parent or legal guardian? If so, how?
iii. If other vulnerable persons' personal data is collected or used for this project, will explicit consent be obtained from their legal guardian? If so, how?

c. Describe alternatives if consent is not feasible:

i. What opportunities will individuals have to decline to provide personal data for this project? If individuals refuse to provide some or all of their personal information, will they be penalized in any way or deprived of a service that the project might otherwise provide? (E.g., additional fees will be charged to cover manual rather than automated processing, individuals will not be able to participate in pilot programs, etc.)
ii. If individuals will *not* be provided with granular choices about how their personal data will be collected and used, why not?
iii. If individual or granular consent is not feasible, can you demonstrate that there is community acceptance or social license for this project's collection and use of personal data? (E.g., surveys or public ballot initiatives, a public hearing or legislative process that reflects that this a legitimate use of data, etc.)

d. Describe individuals' ability to access, correct, and delete, their personal data:

i. Will individuals be given a reasonable ability to access and receive a copy of any of their personal data collected or used for this project? If so, how? If not, why not?

ii. Will individuals be given a reasonable ability to challenge the accuracy of any of their personal data collected or used for this project and have it corrected? If so, how? If not, why not?
iii. Will individuals be given a reasonable ability to request that any of their personal data be deleted and no longer collected or used for this project? If so, how? If not, why not? (E.g., technical requirements, legal or retention obligations, etc.)

V. Data Sharing and Disclosures

a. **Describe any routine sharing of personal data with third parties for this project:**
   i. Describe any regular and intended sharing of personal data from this project to third parties, including which entities will receive the data, what personal information will be shared, for what purpose, and how the information will be shared. (E.g., data could be shared with service providers, with researchers, as part of a publication, with the public, etc., and it could be shared on a case-by-case basis, through bulk transfers of data, APIs, physical files, etc.)
      1. Specifically describe whether personal data will be *routinely* shared with or accessible to: other departments within your organization; other government entities; law enforcement agencies; commercial entities; advertising platforms, data brokers, or information resellers; service providers; researchers; non-profit or community organizations; or the public.
   ii. What controls are in place to prevent or mitigate unauthorized access or use in connection with the sharing of personal data? (E.g., data use limits, contractual commitments not to attempt to re-identify data, audit rights, vendor vetting, encryption in transit, access limits, etc.)
   iii. Will a third party be able to purchase, lease, license, or rent data collected or used for this project (including personal data, aggregated or de-identified data, or partially identified data?)? If so, under what conditions?

b. **Describe how law enforcement or other government entities' requests for personal data will be handled:**
   i. Describe how project staff and partners will respond to non-emergency, non-routine requests from local, state, federal, or international law enforcement agencies to access personal information. (E.g., project team will have discretion to voluntarily share data, data will only be shared when presented with a warrant or other court order, intelligence or cybersecurity threat sharing, etc.)
   ii. Describe how project staff and partners will respond to an *emergency* request from local, state, or federal civil or law enforcement agencies to access personal information? (E.g., what is necessary and proportionate to the situation).
   iii. If personal data collected or used by this project is requested by or shared with law enforcement or another government agency, will individuals be notified of such requests? If so, how and when? (E.g., prior to complying with the request; after providing access to the information; in aggregate, through annual transparency reports, etc.)

c. **Describe how this project will respond to public records or open data requests for personal data:**
   i. Describe to what extent each element of personal data collected and used by this project would be subject to disclosure through public records requests. (E.g., XYZ types of data are clearly covered or exempt; there are colorable arguments to withhold XYZ data; etc.)
   ii. Describe to what extent each element of personal data collected and used by this project might be made public through your organization's open data program.
   iii. Describe how your organization would evaluate and address privacy and re-identification risks prior to publishing datasets from this project.
   iv. If de-identified data from this project is shared, breached, or made public, would access to it "unlock" or establish identifiable links to individuals in other, previously de-identified datasets?

d. **Describe how personal data collected and used for this project will be shared in other circumstances:**
   i. Describe under what conditions personal data will be transferred in conjunction with the reorganization, sale, merger, bankruptcy, sale of assets, or dissolution of your project's organization or its partners or service providers.
   ii. Describe under what conditions, if any, cross-border transfers of personal data to international entities or locations would be expected.
   iii. Describe the extent to which, if any, this project's personal data will be contributed to a data trust, data collaborative, or data commons.

VI. Ethical and Equitable Consideration

a. **Describe how this project's collection and use of personal data will impact particular groups or individuals[5]:**
   i. Is the program *intended* to have a direct impact on certain groups or individuals? Could it be reasonably *perceived* to intentionally impact such groups or individuals? In particular, how would this project's collection or use of personal data impact:
      1. Vulnerable or marginalized communities
      2. People with disabilities
      3. Racial or ethnic groups
      4. Religious groups
      5. People with limited English proficiency
      6. Temporary visitors (tourists, commuters, non-residents, etc.)
   ii. Could this project's collection or use of personal data limit protected political or religious expression by individuals or groups? Could the project's collection or use of personal data chill open discourse or associations?
   iii. Could this project's collection or use of personal data restrict or prevent someone from obtaining particular services or benefits? (E.g., adverse impacts on eligibility for housing, insurance, education, employment, credit opportunities, or other public benefits or services)
   iv. Could this initiative negatively impact individual autonomy and decision-making?
   v. Is any imposition on civil rights and civil liberties brief or extended?
   vi. Is any imposition on civil rights and civil liberties equally distributed, randomly distributed, or focused on particular groups?

b. **Describe how this project's collection and use of personal data will impact the government's influence:[6]**
   i. Would this project's collection and use of personal data increase the authority, control, or influence of the local government over its constituents? Would this project require the government to collect more information about private individuals? Would the project require centralizing personal data that was previously dispersed?
   ii. Would this project's collection and use of personal data increase individuals' insight, influence, and control over the local government?
   iii. Would this project's collection and use of personal data increase the authority, control, or influence of the local government over the private sector?
   iv. Would this project's collection and use of personal data increase the control or influence of the private sector of the local government?
   v. Could this project's collection and use of personal data be perceived as mass surveillance of individuals or communities? (E.g., systemic monitoring of individuals, groups, or public spaces)
   vi. Could this project be repurposed to enable surveillance of individuals or communities or to increase a government entities' authority, control, or influence over individuals? (E.g., municipal ID cards repurposed for federal immigration enforcement)
   vii. If physical devices or sensors are deployed as part of this project, do certain geographic areas appear disproportionately over- or under-represented? Would citizens likely feel like there is ubiquitous surveillance in this area?

c. **How does this project address the potential for data bias and algorithmic discrimination?**
   i. Will the *benefits* of collecting or using individuals' personal data for this project accrue towards one group at the expense of another?
   ii. Will the *risks* of collecting or using individuals' personal data accrue towards one group at the expense of another?
   iii. Will automatic or eligibility decision be made on the basis of individuals' data?
   iv. Is the personal data collected and used for this project appropriately representative of the community? (E.g., does the project unreasonably exclude the personal data of particular groups, such

[5] *Tip: think broadly about who might comprise "particular groups." E.g., students, small business owners, bikers, people experiencing homelessness, protesters, residents of particular neighborhoods, users of particular services, local government staff and employees, etc.*

[6] *Note: Answers that indicate the government's influence will grow or shrink through this project are not necessarily disqualifying, but indicates that additional steps should be taken to earn public trust in this project.*

as persons with disabilities, car drivers, or residents of a particular neighborhood)? Would using inaccurate or incomplete personal information create or reinforce biases towards particular groups or individuals?)

v. If the personal data used for this project were incomplete or inaccurate data, could it foreseeably result in adverse or discriminatory impacts on individuals or groups?
vi. Describe the safeguards this project will use to protect against unfair or discriminatory uses of data. (E.g., disparate impact assessments, routine data quality checks, etc.)
vii. Describe the safeguards this project will use to protect against unfair or illegal bias in algorithmic decision-making. (E.g., right to human review, algorithmic auditing or impact assessments, etc.)

d. Does this project's collection or use of personal data challenge social norms or expectations?[7]

i. Have social norms developed around the use of this technology or the collection of this type of data? If so, how stable or widespread are those norms? Does this project's collection and use of personal data conform to those norms?
ii. Would local communities be shocked or surprised by any particular technology or data use in this project?
iii. Could this project's collection and use of personal data be described as "creepy"?
iv. Does this project engage in any of the following sometimes controversial activities?
    1. Publishing personal data that individuals would be surprised to have made public (such as through open data or public records requests)
    2. Use personal data to evaluate, profile, or score individuals
    3. Use automated decision-making systems that will have legal or significant effects on individuals or groups
    4. Process data on a large scale
    5. Match or combine datasets of personal information
    6. Prevent an individual from exercising a right or using a service (e.g., denying access to a public service because of a refusal to provide personal data)

e. Does this project engage in human subject research?

i. Is a new technology or data use being tested on individuals or groups as part of this project, in the furtherance of generalizable research? If so, describe any informed consent or ethical review process that will be provided by your organization.
ii. Do you have academic or corporate partners in this initiative who will be conducting research as part of this project, or with data from this project? If so, describe any informed consent or ethical review process provided by the academic institution.

VII. Accountability and Oversight

a. Describe the privacy management and training for this project:

i. Are all policies and procedures relevant to the collection and use of personal data for this project fully documented?
ii. Does the organization responsible for this project's collection and use of personal data conduct and document regular assessments of both internal and external privacy risks?
iii. Describe any regular trainings that project personnel and partners will undergo on data privacy and security.
iv. Describe the available budget for data privacy and security for this project.

b. Describe the oversight of this project:

i. Which senior individual within your organization is primarily responsible for how privacy is managed for this project? (E.g., a Chief Privacy Officer, agency or team lead, etc.)
ii. Is there an independent oversight body that is responsible for this project's collection and use of personal data?

[7] *Note: Answers that indicate the collection or use of personal data will challenge social norms are not necessarily disqualifying, but indicates that additional steps should be taken to earn public trust in this project.*

iii. Is there an internal oversight person or organization that is responsible for this project's collection and use of personal data?
iv. Is there an ombudsperson or equivalent role who could be engaged about this project's collection and use of personal data?
v. Describe the process by which project staff or stakeholders (including the public) can submit or escalate reports of potential privacy or ethical violations that occur as part of this project? Are there any whistleblower protections that would apply in the context of this project?

c. **Describe how service providers and partners with access to personal data will be managed for this project:**
   i. Describe how service providers and partners with access to personal data will be supervised and vetted.
   ii. Are service providers' data protection practices audited or supervised on an ongoing basis?
   iii. Will service providers own or have any exclusive rights to individuals' data?
   iv. Will service providers communicate with the public about privacy and security protections? (E.g., in the event of a data breach, an outage or interruption in service, etc.)
   v. Do contracts with service providers:
      1. Require that personal data be protected in a manner consistent with your organization's policies and protections?
      2. Set limitations on the use of personal data?
      3. Prohibit attempts to re-identify individuals?
      4. Require reasonable data security measures?
      5. Provide for the right to audit service providers' data protection measures?
      6. Require all downstream sub-contracts to adhere to the same contractual requirements?
      7. Require notification to your organization of any onward transfer of personal data by service providers or sub-contractors?

d. **Describe any remedies available as part of this project for violations of individual privacy:**
   i. Do individuals have legal rights to redress in the context of this project?
   ii. If the security of individuals' personal data is breached, what, if any, additional redress will be offered to them? (E.g., credit monitoring, restitution, funding of public education and awareness campaigns, etc.)
   iii. If the privacy of individuals' personal data is violated, what, if any, additional redress will be offered to them?