Questions from the Commission on Protecting Privacy and Preventing Discrimination

_____

Companion to Software Application Procurement Principles for Utah Government Entities

Issued February 1, 2021

_____

OFFICE OF THE

STATE AUDITOR

AUDIT LEADERSHIP:

John Dougall, State Auditor

The Commission on Protecting Privacy and Preventing Discrimination

OFFICE OF THE
STATE AUDITOR

Questions from the Commission on Protecting Privacy and Preventing Discrimination

Companion to Software Application Procurement Principles for Utah Government Entities

Office of the State Auditor
Issued February 1, 2021

HOW TO USE THIS DOCUMENT

This document is intended to help government entities within the State of Utah with their procurement of advanced technologies that have the potential to impair the privacy of, or lead to discrimination against, Utahns. The following list of questions and queries are companions to the referenced Principles document. Asking these questions should help government entities improve their evaluation process as they evaluate software vendor offerings and as they issue RFPs or procure commercial software products.

Consider including the questions or queries from the appropriate sections in your RFP and/or RFI and in appropriate proposal scorecards.

These are complex topics and may require subject matter expertise to effectively evaluate proposals. It is suggested that the public entity seek out relevant experts to pose these questions and evaluate the answers.

KEY STEPS

- Identify which sections apply to your particular application. For example, does the application or solution being considered have a potential impact on the privacy of Utahns?
- Could information used or gathered by the solution impact equity and inclusion of Utahns or lead to discrimination?
- Does the vendor use words or phrases that reference artificial intelligence, machine learning, computer vision, surveillance, recording or similar terms?

If so, review the sections below and identify those that apply to your solution.

DEFINITIONS

Artificial Intelligence (AI) - The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. (Oxford Languages via Google Dictionary)

Machine Learning (ML) - A collection of methods used to learn an algorithm for a task from historical data about that task.

Natural-Language Processing (NLP) - Broadly defined as the automatic manipulation and making sense of natural language, like text, by software. (https://machinelearningmastery.com/natural-language-processing/).

Computer Vision - An interdisciplinary scientific field that deals with how computers can gain high-level understanding from digital images or videos.

Public Entity or Government Entity - A state agency, office, board, or commission or a local government entity such as county, city or service district or any political subdivision of the State of Utah, including K-12 education and higher education entities.

PII - Personally Identifiable Information - Information that may lead to an individual being identified. Although there is not a single, universally accepted definition of PII, National Institute of Standards and Technology (NIST) provides a good working definition.[1] "Personally identifiable information (PII) is any information about an individual that is maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information" (based on General Accountability Office and Office of Management and Budget definitions).

[1] NIST, Information Technology Laboratory - COMPUTER SECURITY RESOURCE CENTER
ITL BULLETIN FOR APRIL 2010, GUIDE TO PROTECTING PERSONALLY IDENTIFIABLE INFORMATION,
NIST - https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2010-04.pdf

1. LIMIT SHARING OF SENSITIVE DATA

1.1. What data elements are we considering sharing? Which elements are PII?
1.2 What data is the minimum set of data required to accomplish the task?
1.3 How personal and sensitive is that data?
1.4 Do we need to share that data?
1.5 Do any statutory or policy restrictions or obligations exist? Does the potential recipient understand and agree to these restrictions or obligations? If statutory or policy restrictions or obligations are unclear or non-existent, then the entity should default to caution.
1.6 What expectation of privacy do data subjects have of this data? (e.g. Do Utahns who receive a driver's license expect that data to be used for other purposes?)
1.7 What is the recipient's data retention policy associated with the data? How do we test/verify that they are in compliance?
1.8 How long will the data sharing agreement be in place?
1.9 Who is authorized to share this data (organizational authority)?

2. MINIMIZE SENSITIVE DATA COLLECTION AND ACCUMULATION

2.1 When collecting this data, have we been transparent about how the data will be used? Is there an expectation of privacy on the part of the data subjects?
2.2 Do any statutory or policy restrictions or obligations exist when collecting this data?

2.2.1 Does everyone in our organization who has access to this data understand and agree to these restrictions or obligations?

2.2.2 If statutory or policy restrictions or obligations are unclear or non-existent, then the government entity should default to caution.

2.3 If the data we have collected is shared with a vendor, is there any ability for a vendor, its employees, or its affiliate to download/save data, preserving it beyond normal/approved data retention limits?

2.3.1 If yes, are such events recorded to create an audit trail? How serious is this risk? How serious are the consequences?

2.4. Clearly delineate what data the vendor is receiving and specify the appropriate use of that data.

2.4.1 Have the vendor clearly describe its data retention policies for all key data types as well as for "metadata" (data derived from source data such as video, audio, biometrics, etc.).

2.5 See also section 5.2 Access Provisioning and Management.

3. VALIDATE TECHNOLOGY CLAIMS - INCLUDING CAPABILITY REVIEW

3.1 How will vendor's marketing claims be validated by the government entity during the RFP process and on an ongoing basis? Example claims that warrant particular caution include:

- 3.1.1 Asserted use of AI/ML
- 3.1.2 Proposed use or integration of disparate data sources, including commercially available data, social media or integration of government and private sources
- 3.1.3 Real-time capabilities, especially real-time data intelligence or analysis.
- 3.1.4 Surveillance activities or systems
- 3.1.5 See Section 6. Perform In-Depth Review of AI/ML Algorithms:

4. RELY ON OBJECTIVE, REPEATABLE METRICS

4.1 Are we clear about the problem that we intend for this system or solution to solve for our entity and for our constituents?

4.2 How do we currently solve this problem? What are the strengths and weaknesses of our current solution?

4.3 How do we measure the performance of our current solution? Are we comfortable with sharing our metrics? If not, why not?

4.4 What ongoing metrics will we use to evaluate the effectiveness of this new solution over time? Which of these metrics will the vendor provide and which will the government entity obtain independently?

4.5 How will we decide if the proposed solution is not performing to our expectations or to the expectations of our constituents?

5. ASSESS THREAT MODELS.

System Architecture and Practices to Protect Against Internal or External Malicious Actors or Attacks

5.1 What policies and safeguards exist to protect against a third party actor from intercepting sensitive data?

5.2 Require Vendor to explain their Access Provisioning and Management processes related to:

- 5.2.1 Authorization of access
- 5.2.2 Provisioning

-Does the vendor operate on a least privilege model (minimum required access to accomplish the task)?

-Does the vendor have role-based access with hierarchical permissions?

-What is the vendor's criteria for authorizing administrative/back-end access?

5.2.3 Access Reviews/Auditing

-Does the vendor perform regular access validations and reviews?

-If yes, what is the review cadence or timing?

-What auditing/logging exists for end-user system activity?

-Does the vendor perform audit/log reviews?

-If yes, what is the review timing and frequency?

5.2.4 Access Revocation

-How is access removed and under what circumstances?

5.3. What prevents someone from deliberately introducing bad data (or deliberately skewing the timing or amount of input) to "game" the system or distort outcomes?

General Best Practices in System Maintenance

5.4. Have the vendor describe its baseline system maintenance processes and procedures, describing any third party providers (such as cloud providers or open source solutions) that they use in their system.

Key elements include:

5.4.1 System hardening

5.4.2 Security standards and key management

5.4.3 Data link security

5.4.4 Backup and Recovery

5.4.5 Third party vendors including license compliance

5.4.6 Upgrade, patch, and vulnerability management processes

5.5 Has the vendor had a security breach of its system in the last 5 years? If so, what data was involved and what were the mitigation actions? If so, was there a requirement for regulatory or customer notification?

5.5.1 Have there ever been any simulations to practice a response to a security breach?

6. PERFORM AN IN-DEPTH REVIEW OF AI/ML ALGORITHMS

Many vendors promise that the "magic" of AI/ML will solve complex problems. These technologies are just emerging and generally only specialists are familiar with the details. At the same time, AI/ML can be used poorly, or even abused, and a public entity must evaluate the potential impact of these technologies.

6.1 Have the vendor provide data that validates the claims of their AI/ML system's performance? Where possible, external data or validation should be used.

6.2 Have the vendor provide an overview of the AI algorithms used in the software application and the rationale behind the choice of those algorithms. It is important to remember that AI algorithm choice is closely related to the problem at hand. There is no "single best" AI solution for all problems.

6.3 Have the vendor identify how the outputs of the model are used in different parts of the solution.

6.4 Have the vendor explain the model training and evaluation procedures used in developing the system.

6.5 Have the vendor identify the source and composition of the training, validation, and test datasets. For example, are these commercially available datasets (identify source) or privately developed or proprietary datasets?

6.6 Have vendor demonstrate that it has a license to use datasets.

6.7 Have vendor demonstrate whether the source of training and model data has been evaluated by subject matter experts?

6.8 Have vendor explain pre- and post-processing methods applied to data processes?

6.9 Have vendor explain model lifecycle management, including on-going evaluation

6.9.1 Have vendor discuss whether their model has evolved over time. Does it evolve with system use? How is this managed?

6.10 What data does the vendor have about false positives and false negatives?

6.11 See Section 8 for details on preventing discrimination in the use of AI/ML techniques.

7. DEMONSTRATE PRIVACY COMPLIANCE: PRIVACY SPECIFIC ITEMS AND PROTECTION

7.1 What evidence does the vendor have, and can provide to the government entity, that the privacy protection model is accurate?

7.2 Contracts with government entities sometimes define PII very narrowly (e.g., government-issued identification numbers, financial account information, and personal health information). Have the vendor define PII under the contract. The government entity should also assess whether there are other elements that the entity or the public also consider as PII. Highly sensitive items might be address, phone number, email address, social media handles, demographic information etc. (see broader definition of PII at beginning of document)

7.2.1 What PII is protected in interactions with this vendor? Which elements of PII are removed from which data sources?

7.2.2 If PII about the target person is protected, what about others who might be identified? What about EXIF tags/geotags on images, for example? How is this "non PII" data stored and protected?

7.3 Describe the process for the government entity to verify the vendor's safeguarding of data.

7.3.1 Have any such checks been performed? If so, who performed the verification and how often are they performed? Is this cost built into the contract?

7.4. Have the vendor describe the process by which the vendor anonymizes PII and other relevant data. Where is this done and what are the protections and validations of this process?

7.4.1 Has the vendor considered the problem of de-anonymization of data (see for example, https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable

7.5 What certifications does the application require and what limitations do these certifications have?

8. REVIEW STEPS TAKEN TO MITIGATE THE POTENTIAL FOR DISCRIMINATION

8.1 What evidence does the vendor have, and can provide to the public entity, that the preventing discrimination model is accurate. For example, has a sensitivity analysis (routinely performed on deterministic systems) been performed to know what types of inputs this system is sensitive to?

8.2 What steps has the vendor taken to consider the question of introducing bias that might lead to discrimination within their software application? What mechanisms, such as audit results, does the vendor have to demonstrate that their software application does not disproportionately affect various categories of individuals, particularly any legally protected class (federal, state, or local).

8.3 Does the vendor's system use, rely on, or consider any sources of data that may include implicit or historic bias (e.g., distribution of video cameras by region or neighborhood)? What analysis has the vendor performed?

8.4 Has the vendor evaluated how model choice and training may introduce bias? Have the vendor share such evaluations and conclusions.

8.5 What type of interpretation does the vendor apply to the model output? How might this introduce bias?

8.6 What models has the vendor used to evaluate the risk of discrimination, particularly in the case of biometric analysis or facial recognition?

8.6.1 As an example, NIST provides evaluations of the accuracy of facial recognition based on demographic differences. If such a third party evaluation is available for the vendor's application, has the vendor had its application tested? What are the results?

Note: The output of an AI-based software application may still have issues of bias or lack of fairness, even if the inputs and system are reasonably judged not to include such failings. The output of the software application should be monitored to ensure protection of privacy and avoidance of improper or unexpected bias.

8.7 See also section 6. Perform In-Depth Review of AI/ML Algorithms.

9. DETERMINE ONGOING VALIDATION PROCEDURES TO DEMONSTRATE DATA HANDLING TO PROTECT PRIVACY AND PREVENT DISCRIMINATION

9.1 Are the vendor's data handling practices self-asserted, or are they audited independently? If self-asserted, then the government entity should evaluate the data handling practices. If audited, the government entity should review audit results.

9.2 Is there any mechanism for auditing the quality of anonymization of sensitive data? What is this mechanism? Who conducts these audits? How often are such audits conducted?

9.3 If a particular vendor's system is used by multiple public entities in the State, are all state agencies or public entities that provide or contribute data allowed to see/use one another's data, or is the aggregate view of all these sources illegal or disallowed? Is it or can it be prohibited by contract?

9.3.1 What mechanism exists at the government level to mediate these issues or concerns?

10. REQUIRE VENDOR TO OBTAIN CONSENT OF INDIVIDUALS CONTAINED WITHIN TRAINING DATASETS

10.1 Does vendor have the permission of every individual whose information is contained within its training, validation and test datasets?

10.1.1 Is there any risk that data in its dataset(s) has been "scraped" or otherwise gathered from online sources without the permission of those whose information is included and/or without permission of the owners (who otherwise have permission to use the data)? Have vendor provide credible confirmation of these permissions.

11. VET KEY VENDOR PERSONNEL

The relevance of this section is dependent upon the sensitivity of the data and the implementation model of the technology.

Employee and Founder Background Checks

11.1 Has the vendor conducted intensive background checks of all key employees and founders? What are the factors that would result in employment disqualification?

11.1.1 Are background checks updated on a regular basis? How often?

11.1.2 If key founders or employees have elements in their background that are not consistent with protecting privacy and preventing discrimination, what is our process to address these issues with the vendor?

11.2 Have the vendor provide the "standard" (i.e., template) used by their background check provider.

Vetting Partners and Related Entities

11.3 What other partners help the vendor acquire needed data for the desired capabilities?

11.3.1 Vendor should provide a detailed list of all government entity and private entity partners, along with information on the relevant data sharing agreements. For example, some AI companies have "scraped" social media sites to build their image databases, in violation of social media agreements. All data must be acquired with full permission/ cooperation of the source organizations.

11.3.2 See Section 10.

11.4 If vendor is working with or planning to work with multiple government entities within Utah, a continuously updated master list of all such relationships must be provided to all entities and also to State Purchasing and must be readily available.

11.4.1. "Working with" includes both customer/vendor agreements as well as any data sharing or data access agreements.

12. EVALUATE VENDOR CORPORATE MANAGEMENT, SOLVENCY, AND TRANSPARENCY

12.1 It is often the case with "newer" technology solutions that the company is a startup, privately held, or not yet profitable. Have the vendor provide financial statements and, if the company is not profitable, have vendor provide their financing plan, including the current state of investor commitment.

12.1.1. Review vendor's financial statements and financing history including independently gathering data on the company from "deal reporting" sources such as Crunchbase, Pitchbook, etc. If the company is a startup, privately held, or not profitable, an expert in startup capital should review the cap tables (capitalization tables including details of shareholders and their holdings), and "deal docs" or financing documents to ensure that there are no "poison pills," and no single shareholder that could terminate the company, as well as to ensure financial solvency during the contract period.

12.2 Larger companies should provide written assurances that the proposed product or service will be supported for the proposed project duration. Larger companies are frequently cutting off products and services even when contracts have been signed, leaving government entities without a solution, or required to pay for a new, essentially duplicate, implementation.

12.3 Ensure that a thorough background check has been conducted on each key member of the management team, including key system and technology architects to avoid contracting with a firm who may have malicious actors within the company.

12.3.1 See also Section 11. Vet Key Vendor Personnel

12.4 Conduct a general information search on the company to discover concerns that have been identified.

12.5 Is the vendor transparent about its use of data? For example, are there ways for members of the public to provide feedback and express concerns about the technology, data, and compliance to the governmental entity and/or vendor?

Contract Provisions

12.6 Some contracts include sections that provide for the addition of new modules, components, and other supplementary items being added to the contract after contract signature. The vendor should be required to notify the entity of proposed changes.

12.6.1 All elements of this document may be impacted by the addition of new features or capabilities and so the vendor should be required to address the elements of this document with each new version or upgrade.