Hypothetical NIST Privacy Framework Use Case Profiles

Note to Reviewers

This document is provided for discussion purposes to promote the development of the NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework). In response to stakeholder feedback received on the Privacy Framework Discussion Draft, released April 30, 2019, NIST has prepared these hypothetical use case Profiles to improve understanding of the Core and to demonstrate how the development of Profiles can increase collaboration and dialogue across organizations and support risk-based decisions. NIST is particularly interested in whether these hypothetical use cases: (i) provide greater clarity about the use of the Privacy Framework as an enterprise risk management tool to increase collaboration and communication across different parts of an organization, (ii) demonstrate the Privacy Framework's flexibility, and (iii) whether use cases are the appropriate resource for this role or whether other resources or content within the Privacy Framework should be developed. Please send feedback on this document to privacyframework@nist.gov. NIST will use the feedback to inform the development of a preliminary draft of the Privacy Framework.

Hypothetical Use Case Profiles

As defined in the NIST Privacy Framework Discussion Draft, a *Profile* is "the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, privacy values, and resources of the organization. Profiles can be used to improve privacy posture by comparing a 'Current' Profile (the 'as is' state) with a 'Target' Profile (the 'to be' state)."[1]

Under the Privacy Framework's risk-based approach, an organization may not need to achieve every outcome or activity reflected in the Core, and may create or add Functions, Categories, and Subcategories as needed. To develop a Profile, an organization reviews all of the Functions, Categories, and Subcategories to determine which are most important to achieving its desired privacy outcomes based on industry sector goals, legal/regulatory requirements and industry best practices, the organization's risk management priorities, and the privacy needs of individuals who are directly or indirectly served or affected by—an organization's systems, products, or services. An organization may select Subcategories which it only partially achieves either because it lacks the capabilities to implement all aspects of the outcome or because part of the outcome simply does not apply, given its specific operating context.

The following hypothetical use case Profiles provide examples of how an organization might develop its Profiles using the Ready, Set, Go model in Section 3.4 of the Privacy Framework. There is no set model or format for developing Profiles, so each organization may select what works best for its environment and communications style. Moreover, these hypothetical Profiles are not intended to be comprehensive or cover every Category or Subcategory that an organization might select were these actual use cases; they are designed merely to provide an illustration or snapshot of how the Privacy Framework's Core can be used.

A Simplified Method for Establishing or Improving Privacy Programs

Ready: use the Identify Function to get "ready."

Set: "set" an action plan based on the differences between Current and Target Profile(s).

Go: "go" forward with implementing the action plan.

[1] See NIST Privacy Framework: An Enterprise Risk Management Tool (Discussion Draft) at https://www.nist.gov/document/nist-privacy-framework-discussion-draftpdf.

Example #1: Large Organization in Highly-Regulated Environment

Situation: Company A is a large retail organization with 3000 employees that sells several consumer electronic products, including smart home devices (e.g., garage door openers, thermostats) and wearable devices. It is in the early stages of developing an application for these devices that will allow consumers to 1) register their devices (e.g., for warranty and product update purposes), 2) view information about their usage history, and 3) enable a universal remote control for some of the smart-enabled consumer products in its portfolio (e.g., opening and closing the garage door, adjusting the temperature on the thermostat, recording shows) ("Dashboard App").

Company A has a formalized governance structure in place requiring stakeholder approvals before a product can be released to consumers. The key stakeholders involved in product development are: Senior Management, Product, Marketing, Legal (where the Chief Privacy Officer sits), Chief Information Officer (CIO; the Chief Information Security Officer sits in their office), and Engineering. The Product team, through a Product Manager, is responsible for gathering requirements from the various stakeholders and delivering the requirements to engineers to build capabilities that meet them.

The organization is required to implement and comply with a myriad of privacy laws and regulations both domestic and international. The challenge of navigating complex legal requirements is handled by Legal, and there have been issues in the past where Engineering does not know how to translate legal requirements into system capabilities. Senior Management sees tremendous value in offering consumers a product that enables convenience and remote access to their smart-enabled devices, but also recognizes the potential for privacy concerns, given what the application could possibly collect about their customers' behavior. Company A has seen headlines in the news where other companies were criticized for not paying attention to privacy; its Chief Executive Officer (CEO) is friends with its regional utility CEO and heard about how privacy concerns impeded the rollout of smart meters. Accordingly, Senior Management would like to use the Privacy Framework on the Dashboard App as a test case, to see if they can develop apps in a way that maximizes benefits to their customers and minimizes privacy risk.

READY, SET, GO

Ready: Company A sees that the Privacy Framework recommends that effective privacy risk management requires an organization to understand its business or mission environment; its legal environment; its enterprise risk tolerance; the privacy risks engendered by its systems, products, or services; and its role or relationship to other organizations in the data processing ecosystem. With this in mind, a cross-collaborative team reviews the Identify and Govern Functions first.

- The Legal team is accustomed to considering privacy from a compliance perspective and immediately focuses on the Govern Function, in particular the Subcategory on identifying legal, regulatory, and contractual requirements relating to Company A's privacy obligations.
- The CIO's team already has design artifacts for the Dashboard App's functionality and considers the activities in the Inventory and Mapping Category in the Identify Function to be consistent with, albeit an extension of, their current information inventory processes. Therefore, they can simply overlay a data map on their existing architecture design for the Dashboard App.[2]

[2] NIST has developed a Privacy Risk Assessment Methodology (PRAM) that can help organizations identify, assess, and respond to privacy risks. It is comprised of a set of worksheets available at https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources. See Worksheet 2: Assessing System Design and Supporting Data Map for more information and an example data map.

- The Security team has already been identifying and assessing security risks, such as whether hackers can use the Dashboard App as an entry point to internal systems and confidential corporate information. They review the Risk Assessment Category in Identify and realize that they are not familiar with doing a risk assessment from the perspective of what types of problems the Dashboard App could create for individuals using it.

Set: The CIO's team uses the guidance on creating a data map from the NIST Privacy Risk Assessment Methodology and labels the data actions with icons for different phases of the information life cycle.[3] In a cross-functional meeting, the teams review the CIO's team's data map that shows the different components of the Dashboard App, the owners/operators of the components, and the data actions (system/product/service operations that process data) taking place between the components, including data collection points from individuals, storage of data with a third-party cloud provider, and the databases on which analytics are performed, as well as the specific data elements associated with the data actions.

- The Legal team, having identified a requirement to dispose of data when no longer needed, immediately notices that although there are storage icons on the data map, there are no icons for disposal. This generates a discussion on what data will be stored and for how long. The Legal team, which had not previously focused on the Identify Function, sees that it will need to focus more on the Data Processing Ecosystem Risk Management Category—in particular, the Subcategory on "contracts with data processing ecosystem parties…" to make sure that the contract with the cloud provider includes data disposal provisions. The Engineering team notes that they will also need internal capabilities to manage the disposal of data, including tagging data elements with disposal dates.

- The Legal team has also identified other requirements such as individuals' rights to access and delete data upon request. Engineering takes note of these Subcategories in the Control Function in order to make sure these capabilities are built into all the backend systems. The Security team points out that identity management and authentication will be needed to securely enable these requests. They have built this capability through implementation of the Framework for Improving Critical Infrastructure Cybersecurity—specifically, with the Identity Management, Authentication, and Access Control Category in the Protect Function.[4]

- As the teams continue to review the data map, they realize that compliance requirements have been driving the discussion, but they haven't fully analyzed how to address the fundamental concerns about behavior tracking raised by Senior Management. Under the Risk Assessment Category in the Identify Function, they discuss the likelihood that the different analytic data actions could become a problematic data action of unanticipated revelation and cause their customers to be embarrassed, and what could happen if the analytics service provider used the data for other purposes and whether that could lead to discriminatory decisions by other parties in the data processing ecosystem.[5] They even discuss whether to abandon the Dashboard App after discussing the risks, but an Engineering team member looking at the Data Minimization Category in the Control Function says that it would be nice if they could perform analytics without observing the data. A Security team member remembers a discussion with a friend

[3] Ibid.

[4] See Framework for Improving Critical Infrastructure Cybersecurity at https://doi.org/10.6028/NIST.CSWP.04162018.

[5] NIST has created an illustrative problem set with problems that can range, for example, from embarrassment to discrimination, to economic loss and physical harm), see NIST Privacy Risk Assessment Methodology at https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources. Other organizations may have created additional problem sets, or may refer to them as adverse consequences or harms.

doing cutting-edge research on types of encryption that enable analysis without revealing the underlying data, but Company A would need personnel with specific skills to implement that.

Go: Company A implements the outcomes it selected in the "set" stage, such as those focused on deletion and metadata (see Figure 1 below). Company A ultimately decides to put the privacy-enhancing encryption capability on its action plan to build into the next version of the Dashboard App, and hire a privacy engineer who could implement this technique as well as help it consider other technical measures to mitigate privacy risks.

Results and Impact: When customers ask questions about how their privacy was considered in the development of the Dashboard App, Company A is able to explain the capabilities it developed to enable customers to access and delete data, and measures it is working on to manage additional privacy risks around behavior tracking. When auditors come in to assess for compliance with laws and regulations, Company A is able to show them a copy of its Current Profile and Target Profile, the action plan, documentation on the implementation of the capabilities it built to meet the selected outcomes, and how these artifacts map to specific legal requirements. Communication across the organization is greatly improved and results in a product that took legal requirements and translated them into system requirements and capabilities—and also went beyond compliance to manage additional privacy risks.

Figure 1 below illustrates the relationship of the Functions, Categories, and Subcategories Company A selected for its Current and Target Profiles.

NOTE: Figure 1 provides an example of just a few of the types of Categories/Subcategories that would be within the Profiles for this scenario. In actual use, organizations would likely need additional Categories/Subcategories based upon their business environment.

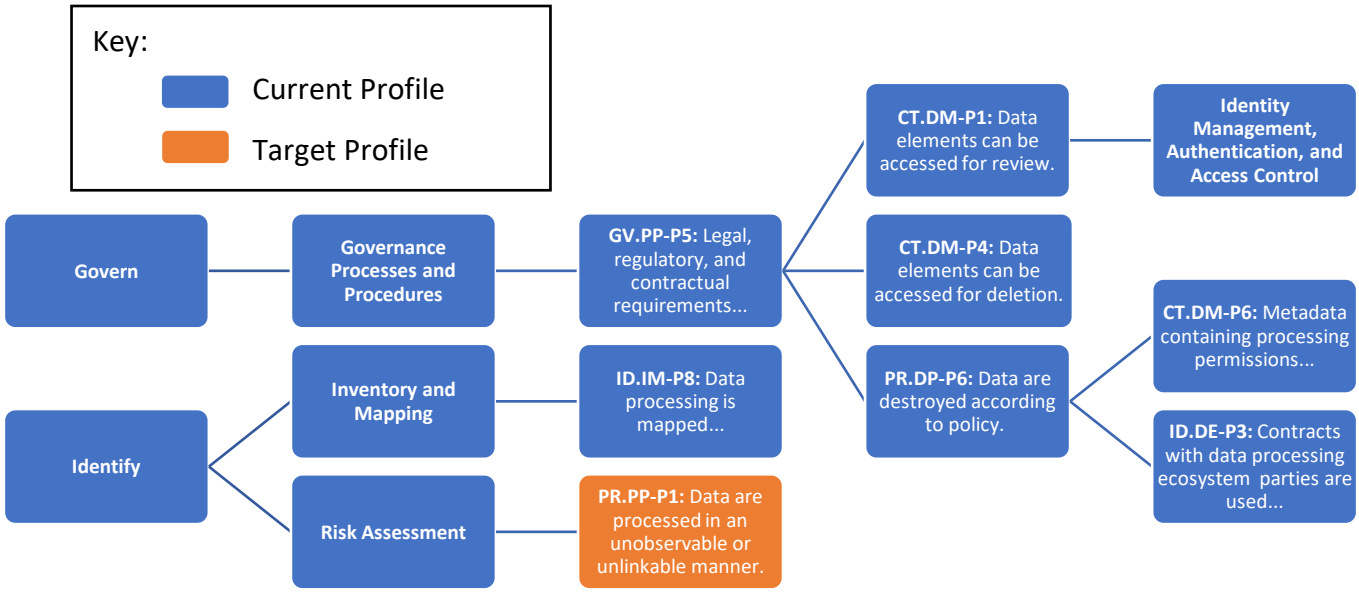

Figure 1: Sample of Company A's Selected Categories and Subcategories

Example #2: Small Business that Develops Mobile Applications

Situation: Company B is a small business (fewer than 15 employees) that develops applications (apps) for many different mobile devices used in a wide variety of industries. Company B's operations are based in the US, but it creates apps used in Europe and Asia. With such a small team, Company B does not have in-house legal counsel, a Chief Information Officer, a Chief Security Officer, or a Chief Privacy Officer. The VP of Engineering at Company B is responsible for all the programmers and oversees all app development processes, filling the de facto information security and privacy roles.

Company B's software engineers and programmers develop the apps based on a set of security requirements provided by Company B's clients. This process is coordinated by a Product & Client Manager, who has multiple responsibilities; while neither a security nor privacy expert, the Product & Client Manager has an awareness about the importance of privacy and security for building trust.

Increasingly, clients are asking Company B to build in specific privacy and security controls, and to develop apps that are compliant with a wide range of privacy and security laws and regulations. Company B wants to, in the short-term, demonstrate that its apps are compliant with these privacy laws. The CEO—in conjunction with the Product & Client Manager and the VP of Engineering—decides that the current practice of addressing privacy according to client-identified data security requirements is no longer sufficient. Proactively considering compliance with existing laws is an important start; in the long term, Company B wants a more robust privacy program to address emerging privacy laws and manage risks that arise beyond legal obligations.

Company B's CEO and VP of Engineering decide that since they currently have no workforce members with privacy experience, they need to engage outside help to create a privacy program, so they contract a privacy consultant. The consultant, in conjunction with Company B's CEO, decides to use the NIST Privacy Framework, which they determine will demonstrate due diligence and serve as a marketing differentiator from their competitors. It will also serve as a helpful communication tool since it's accessible to both privacy and non-privacy professionals, and Company B interacts with a wide variety of different skillsets in client discussions (e.g., lawyers, C-suite, engineers).

READY, SET, GO

Ready: The consultant works with a various teams in Company B as she uses the Privacy Framework: the VP of Engineering, who has accountability for the privacy of the apps, and the app engineers, programmers, and the Product & Client Manager.

After interviewing these key stakeholders, the consultant determines that the best first step is to establish a set of core privacy practices to address the short-term needs, including immediate client requests. The VP of Engineering, eager for clearer ways to track Company B's progress, signs off on the consultant's plan to build a Current Profile focused on app development, and a Target Profile for where Company B wants its app development program to be. In considering the app development program, the consultant and VP of Engineering scope the Profiles to the three following processes: app design, app engineering and coding, and app testing. The plan is to replicate this Profile development process for the rest of Company B's business operations by next year.

- In building Profiles for the app development program, the consultant first focuses on the Identify and Govern functions. She assesses the priority obligations of Company B by reviewing requirements lists from clients, along with identifying laws in the jurisdictions and sectors in which Company B's apps are currently used. By achieving selected outcomes in the Identify and Govern functions, Company B is able to meet its immediate needs while also laying the foundation for a more robust, organization-wide privacy program in the future.

- Given the lack of privacy expertise in Company B, the consultant selects several outcomes from the Awareness and Training Category in the Govern Function, to not only ensure that Senior Management at Company B understands their roles related to privacy—but also to prioritize basic privacy awareness training company-wide.

Set: With the roles and responsibilities, legal requirements, and client requests identified, the consultant now selects additional Privacy Framework Functions, Categories, and Subcategories to fill out the Current Profile.

- Several clients have requested more opportunities for their customers to participate in the app's configuration, as it relates to the processing of their data. With this in mind, two Subcategories that stand out to the consultant: CR.PO-P3, about policies, processes, and procedures for data management, and CT.MN-P6, about selective collection or disclosure of data elements.
- The consultant is also particularly interested in CM.PP-P1, as many of the clients have legal obligations related to privacy notices for their customers and have been asking for support from Company B in defining transparency methods.

Go: Company B implements the outcomes it selected in the "set" stage. Company B decides to wait until later in the year to do a full risk assessment. For now, the VP of Engineering is most concerned with client requests and legal obligations; months from now, they'll do a risk assessment to identify risks that arise beyond this. Thus, they choose the risk assessment-related Subcategories for the Target Profile.

Results and Impact: When clients make inquiries to Company B about the capabilities for creating apps to provide privacy choices to their customers and to support their legal requirements, Company B provides consistent and accurate responses, using the functions to communicate at a high level how they incorporate privacy into app development. Company B is sending a newsletter with all current clients highlighting forthcoming privacy efforts, using Subcategories from the Target Profile to share specifics of future work. Company B also plans to share the Profiles with auditors and regulators.

In discussions with potential clients, Company B is beginning to share a few of the benefits of its privacy-enhancing approach:

- Customer satisfaction, engagement, and trust leading to more clients and client retention
- Compliance with legal requirements based on organizations' jurisdiction and sector
- Reduction of noncompliance risks
- Mitigation of some potential privacy problems, lessening the likelihood of a privacy event

Table 1 shows a sample of a few of the Categories and Subcategories used to define the Profiles for the actions identified throughout the project.

NOTE: Table 1 provides an example of just a few of the types of Categories/Subcategories that would be within the Profiles for this scenario. In actual use, organizations would likely need additional Categories/Subcategories based upon their business environment.

Table 1: Sample of Company B's Selected Categories and Subcategories

Function	Category	Selected Subcategories	Current Profile	Target Profile
Govern (GV-P): Develop and	**Governance Policies, Processes, and**	**GV.PP-P2:** Processes to instill	Company B does not have any documented, or regularly verbalized, privacy	Policies, processes, and procedures have been created, vetted, and implemented to

Function	Category	Selected Subcategories	Current Profile	Target Profile
implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Procedures (GV.PP-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	organizational privacy values within system/product/service development and operations are established and in place.	values.	promulgate privacy values throughout the entirety of Company B.
		GV.PP-P3: Roles and responsibilities for the workforce are established and in place with respect to privacy.	Company B has assigned privacy-related roles at a high level. a. The role with privacy accountability is the VP of Engineering. b. The roles with privacy responsibilities are app engineers and programmers, and the Product & Client Manager.	Roles and responsibilities related to privacy have been incorporated into the documented job descriptions and annual performance plans.
		GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	a. Identifying the legal and regulatory requirements for app use in all jurisdictions and sectors in which Company B clients operate. b. Documenting the requirements in a form understandable to those with responsibilities for implementing privacy controls within the apps.	a. Company B has done an analysis of contractual requirements of their clients, which might extend beyond legal obligations. b. Company B has done an analysis of emerging legal and regulatory requirements in jurisdictions and sectors in which clients currently operate. c. Company B has done an analysis of legal requirements in new regions Company B would like to enter.
	Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are	**GV.AT-P1**: The workforce is informed and trained on its roles and responsibilities.	a. Certain roles (not all) in Company B are aware of how privacy relates to their role; for instance, the VP of Engineering is accountable for privacy in apps. d. No validation is made to	a. Procedures are established and consistently followed for providing consistent privacy training and frequent reminder messages to the engineers and programmers for privacy in app

Function	Category	Selected Subcategories	Current Profile	Target Profile
	provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.		ensure programmers understand privacy implications of the apps they design and build.	development. b. All workforce members that take the training are logged, and VP of Engineering approved methods (e.g., quizzes on the training topic) are used to verify that those taking the training understand the topics it covers.
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	a. Privacy requirements are included within contracts in an ad hoc manner, and sometimes not included at all, with third parties that support aspects of app development. b. It is left to the contracted third party to provide any training to their workers for any contractually required privacy requirements.	a. Procedures are established and consistently followed for ensuring all requirements for developing apps with acceptable privacy protections are included in every contract with third parties that are used to support app development activities. c. Procedures are established and consistently followed for obtaining reasonable documented assurances (e.g., executive attestations, training documentation) from the third parties that their workers have been made aware of, understand, and will follow the requirements.
Identify-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from system, product, or	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services are understood and inform the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.	a. Existing apps that include access to personal data, or that could reveal information about people's lives, are not consistently documented in data maps. Those that are documented aren't all in the same format and don't all include the same information. b. As new apps are	a. Procedures have been implemented and are consistently followed to document privacy considerations for new apps and updates to existing apps that involve processing of data. b. Procedures are followed to consistently document and inventory data actions and associated data elements, and roles of component

Function	Category	Selected Subcategories	Current Profile	Target Profile
service data processing.			developed, each development team determines on an ad hoc basis what to document with regard to the processing of individuals' data, if anything.	owners/operators.
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, developers, etc.) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	a. The VP of Engineering is accountable for privacy in apps, and currently considers privacy requirements based on what is communicated by the clients to the Product & Client Manager. b. No formal documentation exists identifying responsibilities for communicating privacy requirements to the engineers and programmers building, testing, and maintaining the apps. The Product & Client Manager provides information from each app client that may or may not include privacy requirements for existing apps and new apps being developed.	a. The VP of Engineering role expands to incorporate proactive privacy, rather than being purely reactive to client requests. b. Privacy responsibilities are established for app development teams (engineers and programmers). This include requirements for incorporating privacy controls and features within each app, appropriate to each app project, that are documented, implemented, and consistently followed. c. Responsibilities and procedures are established for the Product & Client Manager to consistently obtain information from app clients for privacy requirements for each app development project.
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create secondary impacts on organizational	**ID.RA-P3:** Potential problematic data actions and associated problems are identified**.**	Company B is not currently doing a risk assessment; rather, the company is focusing on complying with client requests, and laws and regulations.	Prior to coding, the design for each app will be assessed to identify potential privacy risks engendered by processing data.

Function	Category	Selected Subcategories	Current Profile	Target Profile
	operations (including mission, functions, reputation, other risk management priorities (e.g. compliance, financial), workforce, and culture).			
Control-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.	**Data Minimization (CT.MN-P):** Technical data processing solutions increase disassociability consistent with related policies, processes, procedures, and agreements and the organization's risk strategy to protect individuals' privacy.	**CT.MN-P6:** System or device configurations permit selective collection or disclosure of data elements.	Company B does not currently enable selective collection or disclosure of data elements in its app designs. Thus, in order to use the apps, customers must provide a bundle of attributes at the client organization's request—some of which may not be required to operate the app.	Company B designs apps in a way that permits selective collection or disclosure of attributes, giving users choice in what data they provide and to whom. To facilitate this process, the Product & Client Manager asks the client in initial design conversations to indicate which attributes are required, and which are optional for individuals to provide (i.e. not critical to operation of the app).
	Data Management Policies, Processes, and Procedures (CT.PO-P): Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles, responsibilities, management	**CT.PO-P3**: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	The Product & Client Manager typically recommends to the client leaving certain components of the app configurable so individuals have some say over how their data is processed. This is done informally in initial discussions with the client, and the suggestions from the Product & Client Manager are different each time.	In the early stages of discussing app design, the Product & Client Manager works with the VP of Engineering to identify several opportunities to enable user preferences, and provides a written list of options to the client. This written list includes both basic and more complex options, and each option is listed beside the risks it could help manage, and the cost of implementation.

Function	Category	Selected Subcategories	Current Profile	Target Profile
	commitment, and coordination among organizational entities) consistent with the organization's risk strategy to protect individuals' privacy.			
Communicate-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PP-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) and associated privacy risks.	**CM.PP-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	Currently the only information made available to app users is the type of privacy notice clients indicate they want to make available through the app. There is no formally established set of communication options for communicating purposes, practices, or privacy risks in place.	a. App development teams consistently follow an established set of processes and procedures to define the types of transparency methods that will be made available to clients, that are in compliance with identified legal requirements. b. As legal requirements expand, new processes and procedures will be added as needed, and procedures will be updated accordingly.

217