The following hypothetical use case Profile provides an example of how an organization might develop its Profiles using the Ready, Set, Go model in Section 3.3 of the NIST Privacy Framework. This hypothetical use case is not intended to be comprehensive or cover every Category or Subcategory that an organization may select in a given scenario; it is designed merely to provide illustrations of how the Privacy Framework Core could be used.

# Hypothetical Use Case #2: Small Business without an Established Privacy Program

## 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 (they hire outside counsel, as needed), a Chief Information Officer, a Chief Information Security Officer, or a Chief Privacy Officer. The VP of Engineering at Company B is responsible for all the programmers, oversees all app development processes, and fills the cybersecurity 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 of the importance of privacy and security for building trust, and uses outside counsel to consult on applicable laws and regulations.

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 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 various teams in Company B as she uses the Privacy Framework: the VP of Engineering, who has accountability for the privacy posture 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 app development program goals. 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 stand out to the consultant: CT.PO-P3, about policies, processes, and procedures for data management, and CT.DP-P4, about selective collection or disclosure of data elements.
- The consultant is also particularly interested in CM.PO-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. In the immediate term, the VP of Engineering is most concerned with client requests and legal obligations; then they'll do a risk assessment to identify risks that arise beyond this. Thus, they choose the entire Risk Assessment Category for the Target Profile.

**Results and Impact:** When clients make inquiries to Company B about creating apps that provide privacy choices to their customers and 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 to 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 selected Functions/Categories/Subcategories for a Current and Target Profile for this scenario. It is not intended to demonstrate a complete set of Profiles.**

**Table 1: Excerpt of Company B's Current and Target Profiles**

| Function | Category | Selected Subcategories | Current Profile | Target Profile |
|---|---|---|---|---|
| **Govern (GV-P):** Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk. | **Governance Policies, Processes, and Procedures (GV.PO-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. | **GV.PO-P2:** Processes to instill organizational privacy values within system/product/service development and operations are established and in place. | Company B does not have any documented, or consistently verbalized, privacy values. | Policies, processes, and procedures have been created, vetted, and implemented to promulgate privacy values throughout the entirety of Company B. |
| | | **GV.PO-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.<br>a. The role with privacy accountability is the VP of Engineering.<br>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 documented job descriptions and annual performance plans. |
| | | **GV.PO-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.<br>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.<br>b. Company B has done an analysis of emerging legal and regulatory requirements in jurisdictions and sectors in which clients currently operate.<br>c. Company B has done an analysis of legal requirements in new regions Company B would like to enter. |
| | **Awareness and Training (GV.AT-** | **GV.AT-P1**: The workforce is | a. Certain roles (not all) in Company B are aware of | a. Procedures are established and consistently followed |

| Function | Category | Selected Subcategories | Current Profile | Target Profile |
|---|---|---|---|---|
| | **P):** The organization's workforce and third parties engaged in data processing are 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. | informed and trained on its roles and responsibilities. | how privacy relates to their role; for instance, the VP of Engineering is accountable for privacy in apps.<br>d. No validation is made to ensure programmers understand privacy implications of the apps they design and build. | for providing consistent privacy training and frequent reminder messages to the engineers and programmers for privacy in app development.<br>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.<br>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.<br>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 | **Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services are | **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 | a. Procedures have been implemented and are consistently followed to document privacy considerations for new apps and updates to existing apps that involve |

| Function | Category | Selected Subcategories | Current Profile | Target Profile |
|---|---|---|---|---|
| privacy risk for individuals arising from system, product, or service data processing. | understood and inform the management of privacy risk. | | maps. Those that are documented aren't all in the same format and don't all include the same information.<br>b. As new apps are developed, each development team determines on an ad hoc basis what to document with regard to the processing of individuals' data, if anything. | processing of data.<br>b. Procedures are followed to consistently document and inventory data actions and associated data elements, and roles of component 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.<br>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.<br>b. Privacy responsibilities are established for app development teams (engineers and programmers). This includes requirements for incorporating privacy controls and features within each app, appropriate to each app project, that are documented, implemented, and consistently followed.<br>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 | **ID.RA-P3:** Potential problematic data actions and associated | Company B is not currently doing a risk assessment; rather, the company is focusing on complying with client requests, and laws | Prior to coding, the design for each app are assessed to identify potential privacy risks engendered by processing data. |

| Function | Category | Selected Subcategories | Current Profile | Target Profile |
|---|---|---|---|---|
| | individuals and how such privacy risks may create secondary impacts on organizational operations (including mission, functions, reputation, other risk management priorities (e.g. compliance, financial), workforce, and culture). | problems are identified**.** | and regulations. | |
| **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 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 commitment, and coordination among organizational entities) consistent with the organization's risk strategy to protect individuals' privacy. | **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 |
|---|---|---|---|---|
| | **Disassociated Processing (CT.DP-P):** Data processing solutions increase disassociability consistent with related policies, processes, procedures, and agreements and the organization's risk strategy to protect individuals' privacy. | **CT.DP-P4:** 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). |
| **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.PO-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.PO-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.<br>b. As legal requirements expand, new processes and procedures will be added as needed, and procedures will be updated accordingly. |