The following hypothetical use case 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 Function, 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 #1: Compliance-oriented Large Organization

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), and Engineering. The Product team, through a Product Manager, is responsible for gathering requirements from the various stakeholders and delivering the requirements to engineers who will then 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; 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 both maximizes benefits to their customers and minimizes adverse consequences.

READY, SET, GO

Ready: Company A reads in the Privacy Framework that effective privacy risk management begins with an organization understanding 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-P and Govern-P Functions first.

- The Legal team is accustomed to considering privacy from a compliance perspective and immediately focuses on the Govern-P 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-P Function to be consistent with, albeit an extension of, their current data inventory processes. Therefore, they can simply overlay a data map on their existing architecture design for the Dashboard App.[1]
- 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 information on creating a data map from the NIST Privacy Risk Assessment Methodology, labeling the data actions with icons for different phases of the data life cycle.[2] 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. The data map notates the 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.[3]
- 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. They also discuss what could happen if the analytics service provider uses the data for purposes other than what's

[1] 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.

[2] Ibid.

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

originally intended, and whether that could lead to discriminatory decisions by other parties in the data processing ecosystem.[4] They even discuss whether to abandon the Dashboard App after discussing the risks, but an Engineering team member looking at the Disassociated Processing Category in the Control Function identifies certain subcategories that could reduce the risk to an acceptable degree; this team member 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 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. These measures help the Company better articulate its privacy practices in both its privacy policies and notices for the App. Marketing materials now prominently feature privacy-enhancing attributes of their product allowing privacy to be a market differentiator. 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 translates legal requirements into system requirements and capabilities—and also goes 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 selected Functions/Categories/Subcategories for a Current and Target Profile for this scenario. It is not intended to demonstrate a complete set of Profiles.

[4] 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.

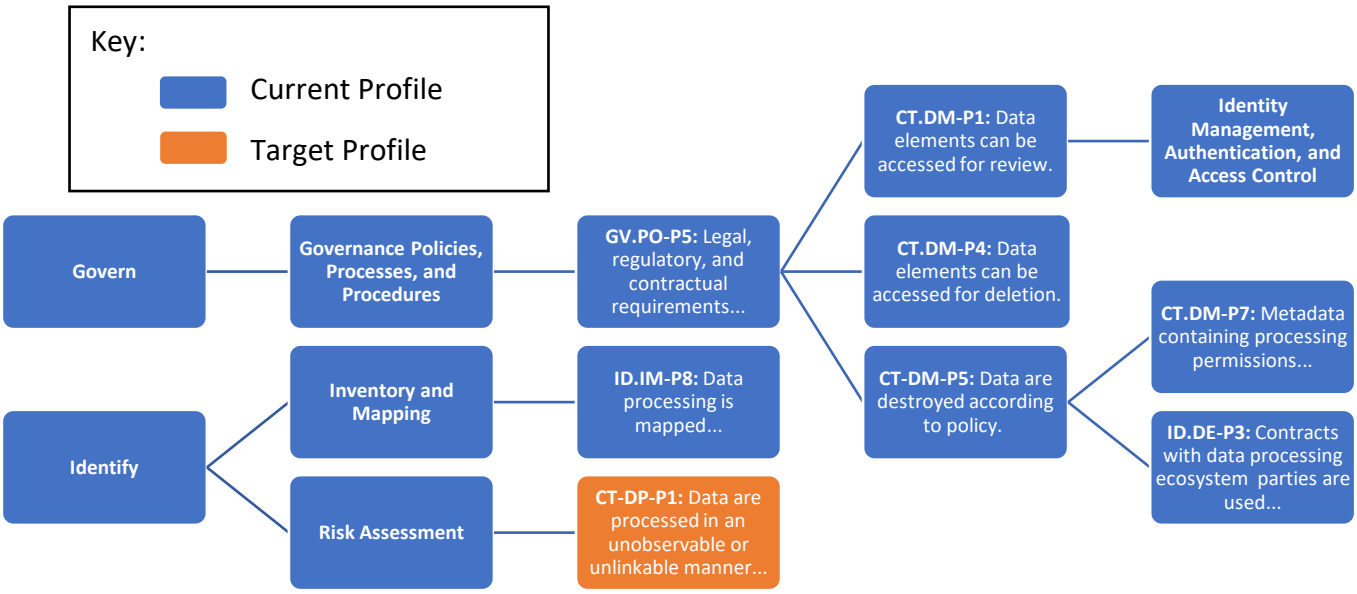

Figure 1: Excerpt of Company A's Current and Target Profiles