CHAPTER 7

# The Privacy Component App

This chapter describes a primary tool in the privacy engineer's toolkit, the privacy component, originally introduced in Chapter 5. The privacy component is a self-contained, reusable software building block module developed to satisfy the privacy requirements derived from the use case discussed below. It is recommended that this component be developed as a module that can be used standalone or plugged into another enterprise program or mobile app, as will be discussed later in this book.

The privacy component should be developed according to the privacy engineering methodology, as described in Chapter 6. It will ensure that personal information is collected according to privacy policies and will be used to maintain the Privacy Notice as per the use case. The privacy team, along with the data stewards, will enter and maintain the privacy rules. The privacy component will determine the role of the person impacted and then execute the appropriate privacy rules. Encryption and security subcomponents are invoked, as appropriate, by the privacy component, according to the privacy rules.

## Privacy Component Context Diagram

Figure 7-1 presents a context diagram for the privacy component.

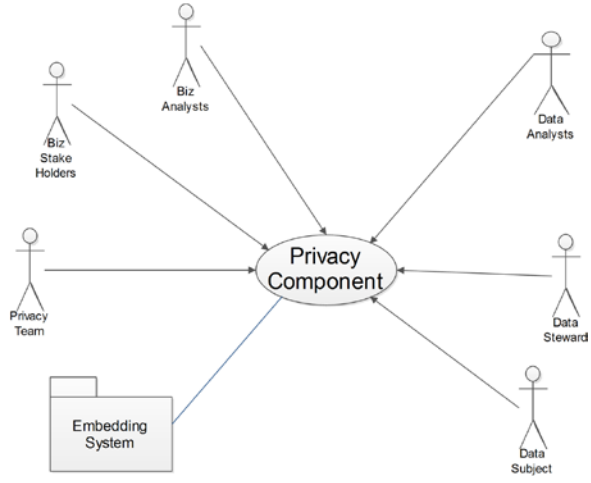



***Figure 7-1.*** *Privacy component context diagram*

Privacy team members ensure that the privacy rules are entered into the metadata repository according to the privacy policies established, as discussed in Chapter 4. The business analysts and business stakeholders utilize the data governed by the privacy rules. The data analysts may analyze the data but also support the data stewards in adding privacy-oriented metadata. The data subjects are both impacted by the privacy component and use the privacy component directly via the user interface. The embedding system interacts with the privacy component via an application program interface (API).

## Use Case Requirements to Build a "Privacy Component"

A use case can be used to gather and document privacy requirements, as discussed in Chapter 5. The privacy component will satisfy the requirements as discussed in this section. These requirements will be documented in the use case documentation or documented in a metadata repository.[1] When developing the requirements, six analytical questions are asked:

- *Why*: The privacy component mission based on the requirements developed in this section
- *Who*: The privacy stakeholders, as depicted in the context diagram in Figure 7-1 (organizational aspects of the roles are discussed in Chapter 12):
    - Privacy executives and other privacy team members, who should ensure the requirements of the enterprise's privacy policy are understood and met, including requirements based on relevant laws and regulations
    - Business stakeholders, who, along with data stewards, must represent the end-user community (e.g., employees and parents) as well as business interests
    - Business analysts
    - Data analysts
    - Data stewards, who represent and may also be data subjects or advocates themselves
    - Data subjects, who share or are the subject of data collection and processing
- *When*: The privacy component triggering events:[2]
    - Data subject events:
        - Need to provide the data subject's data to the subject

[1] See further discussion of this in Chapter 6 and Appendix A.
[2] A triggering event is one that causes decision processing that uses business rules, including privacy rules, as decision criteria and triggers a behavior.

        - Need to allow a data subject to correct his or her own data according to privacy rules
        - Privacy notice needed
        - Ability to gain the consent needed and manage changes within the model
    - PI-related events:
        - Need to collect PII and related data to maintain, store, test, or deactivate these data
        - PI and related data to be presented to user
        - PII need to be transferred or transformed with metadata
        - Machine or other non-PII to be transformed to PII upon combination with other data elements or combinations with additional systems
    - Privacy component internal events:
        - Need to create or update privacy rules
        - Need to transfer data to third party
        - Need to determine archive rules
        - Need to invoke encryption or obfuscation or other data limiting or masking technology solution
- *How*: The information privacy component behavior processes invoked by triggering events
    - Data subject related:
        - The Privacy Notice should be presented by means of an interactive user interface so that the end user can choose whether to read the notice.
        - Data subject must be able to agree to the storage of his or her data and needs to understand how these data will be used.
        - Data subject must be able to review his or her data.
        - The data subject should be able to correct any incorrect data.
    - Data collection related:
        - Must be the minimum relevant requirement needed to support the services provided
        - Must be proportional to the need

    - Privacy component internal behaviors:
        - The user interface must contain a security component, including authentication and authorization.
        - Archiving rules need to be executed.
        - Encryption must be available as needed.
- *What*: The information privacy component data:
    - Privacy policies reflecting legal, cultural, and enterprise requirements (as discussed in Chapter 4)
    - Privacy business[3] rules
    - Individual role
    - Enterprise role
    - Organization
    - Individual person
    - Interface mechanism between the privacy component and an embedding system that may be used for adding or updating privacy rules. Another use is to present the Privacy Notice and allow an end user to choose whether his or her data are collected.
- *Where*: Locational aspects, depending upon where the enterprise operates and how distributed the enterprise network is. These considerations are particularly important for transborder data flows, where multijurisdictional rules or policies may apply, or where end users or other third parties may require an audit or limitation on data flows.

# The Privacy Component Class Model

We use the UML class model as both a class model and a data model, as mentioned in Chapter 6. A UML class model is *not* a data flow diagram. Instead, a class model shows the relationship (or association) of the classes to one another. In Figure 7-2, the arrow-like symbol shows class inheritance. For instance, an organization and an individual person are subtypes of persons of interest and inherit attributes from the person of interest super-type. The diamond-like icon indicates an aggregation, whole-part, or one-to-many association. For instance, each role can have one or more privacy rules relationships, and the various rules may have overlapping origins as well.

[3]In this case, "business" rules cover any type of organizational activity rules. These are not exclusive to commercial enterprises.

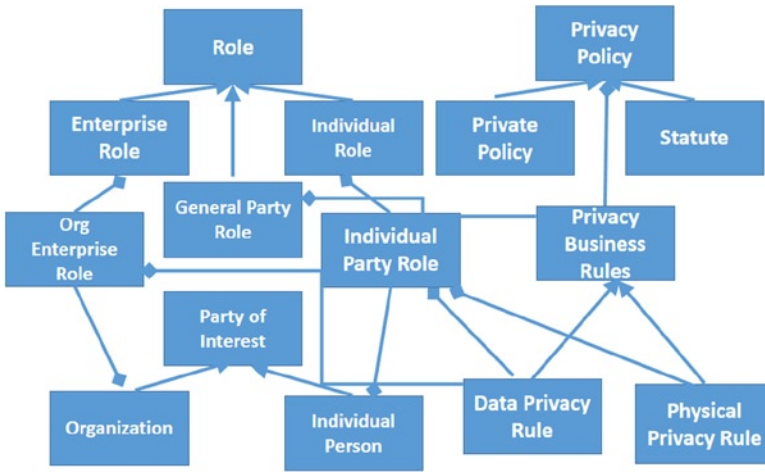



***Figure 7-2.*** *Privacy component class model*

A class also has knowledge properties (data) and action properties (event handlers and processes). Each of these classes will have both class and operational metadata attributes. Class attributes are data elements that describe aspects of that class. A class that describes one of the privacy policy requirements may have a uniqueness identifier, a name, and a text description. Operational metadata attributes are names of operations that are also the names of code modules or services to be invoked according to embedded rules implied by requirements.

## Developing the Unified Modeling Language Class Model

The class model, like a data model, shows the data that will be managed and the relationships between the various classes.

The privacy component class model graphic in Figure 7-2 shows *classes* that represent data managed by the enterprise and the data privacy requirements. The privacy component is composed of parties of interest, roles, policies, and rules. The party of interest subcomponent (lower left corner of Figure 7-2) was described in detail in Chapter 6.

Roles (upper left corner subcomponent) may be defined as the nature of work performed by an individual person or organization with regard to enterprise functions. General party roles, as opposed to individual or enterprise roles, may be relevant to a party of interest whether they are an individual person or an organizational entity. An individual can have one or more individual roles as mapped through the individual party role and an organization can have one or more enterprise roles as mapped through the organization enterprise role.

Privacy policies (upper right corner) may be statutory or a policy developed and enforced by private entities, as described in Chapter 4. Privacy policies contain the basis for privacy business rules or requirements.

Privacy business rules can be defined as written statements in natural language that function as a communication tool to express a rule, decision criteria, policy, or a common practice in relation to a decision involving business information or business processes. They can be data or physical privacy rules. Privacy rules are mapped across the diagram to the individual party, organization enterprise, and general party roles. Note that general party roles may be related to surveillance or other aspects of party of interest physical privacy as well as data privacy per se, but it is the data about that protection that will require policy creation, execution, and monitoring for both individuals and organizations.

# Privacy Component User Interface Requirements

The privacy component and the system or application in which it is embedded will need to protect the integrity and security of the data subject's data. Some aspects of the user experience may be balanced with the requirements under privacy legal and regulatory schema to protect information with security techniques. Often, in development environments, additional steps or required processes may be deemed a diminution of overall user experience. When the overall architectural aspects are managed in a privacy engineering data and user-centric environment, security protocols are also managed and contextual cues and other aspects of user experience design are utilized to effectively engage the user.

A Privacy Notice describes to the user a summary of enforcement and redress relevant to the privacy-oriented information related to the system. The user experience and Privacy Notices can themselves be deemed privacy-enhancing technologies. They may set and expand context and set a tone of expectation for the user. They also may function to provide clear guidance to the privacy governance professional who will serve as the fiduciary of data processes within the architecture. This is where an innovative animated notice enhances both the user experience and the data subject protection.

The system user, whether of the standalone privacy component or of an application that invokes the privacy component, interacts with the privacy component. If the privacy component is invoked, the user should not have to know that the invocation has occurred. Instead, a seamless transition should happen between the overall system and the privacy component.

The data steward, supported by the privacy team and the data analyst, ensures that the privacy rules are entered. The privacy team representative enters and maintains the Privacy Notice. The user of the system will interact with the system invoking the privacy component, utilizing that system's functionality. The privacy component will mostly operate behind the scenes.

# Design the Privacy Component Solution

## The Privacy Component Solution Architecture

The privacy component use case lays out the requirements for developing a privacy component that can be invoked by an enterprise application to ensure that privacy policies are enforced, as discussed in Chapter 5 and previously in this chapter. The privacy component class model provides the basis for the information architecture (Figure 7-3) and defines a series of events requiring a user interface architecture.

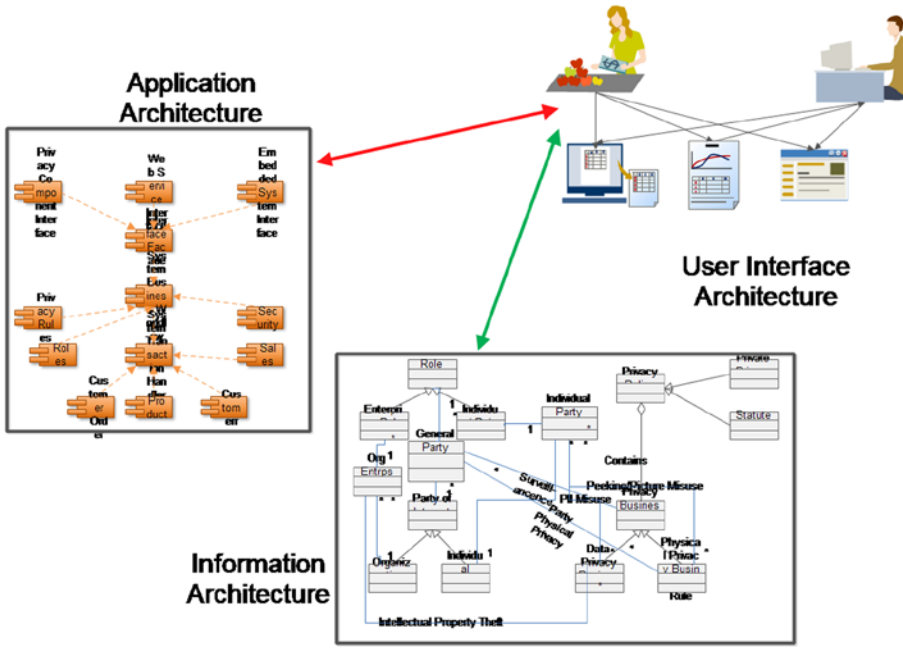



***Figure 7-3.*** *Solution architecture*

Examples of user interface requirements include:

- The ability to request the Privacy Notice
- The display of the notice, if requested
- The ability to add and maintain privacy rules related to the roles shown in the metadata model

The application architecture is developed by following the component design methodology, as described in Chapter 6.

## The Privacy Component Class Structure

We can best understand how the privacy component might work by analyzing the component metadata model (Figure 7-4). The privacy component may be embedded in a system (as a component within an application), as we discussed regarding scenarios 2 and 3, or as a mobile app (itself) or program subroutine (code within the application), or it may invoke a more broad-based system in the Cloud.

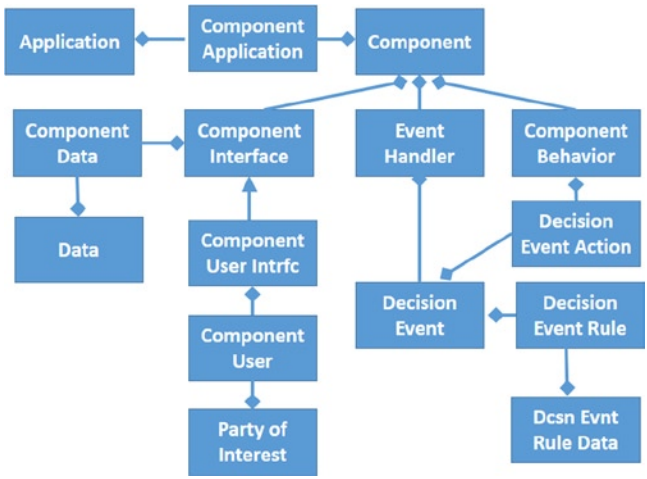



***Figure 7-4.*** *Component metadata model*

The component interface may utilize a database (component data) based on the privacy component data model shown in Figure 7-2, and, in most cases, it may also utilize the database for the system it is embedded within (e.g., the simplified customer order data model [scenario 3], as discussed in Chapter 9). The component interface has a user interface for interacting with the privacy component actors shown in the context diagram in Figure 7-1.

The privacy component event handler will process the events listed as the privacy component triggering events in the privacy component use case requirements. Each event implies one or more decision to be made. For instance, the user interface will ask the user if he or she wishes to see the Privacy Notice.[4] When the user gives an affirmative answer, it invokes one set of privacy rules, and a negative answer invokes another set of privacy rules based on the role of the user.

Thus, each event triggers one or more decisions, and each decision requires a set of privacy rules as the criteria for making the decision. Each decision will then invoke a process or behavior that may trigger another event, and its decision sets or may invoke another behavior all in accordance with the privacy rules. Each of the privacy rules may require access to a database related to the privacy component.

## Privacy Component System Activity Diagram

The system activity diagram in Figure 7-5 shows where the major actors interface with the privacy component system functionality as defined by the use case and implied by the data requirements. The functionality is grouped into modules or subcomponents: The first subcomponent may be considered administrative in nature; the second subcomponent is for initiation and data collection; the third subcomponent handles third-party transfers; the fourth subcomponent manages data correction; and finally, there is the archive rules subcomponent.

[4]FIPPS/GAPP requires that a Privacy Notice that defines the enterprise's privacy policies be made readily available to a system user.

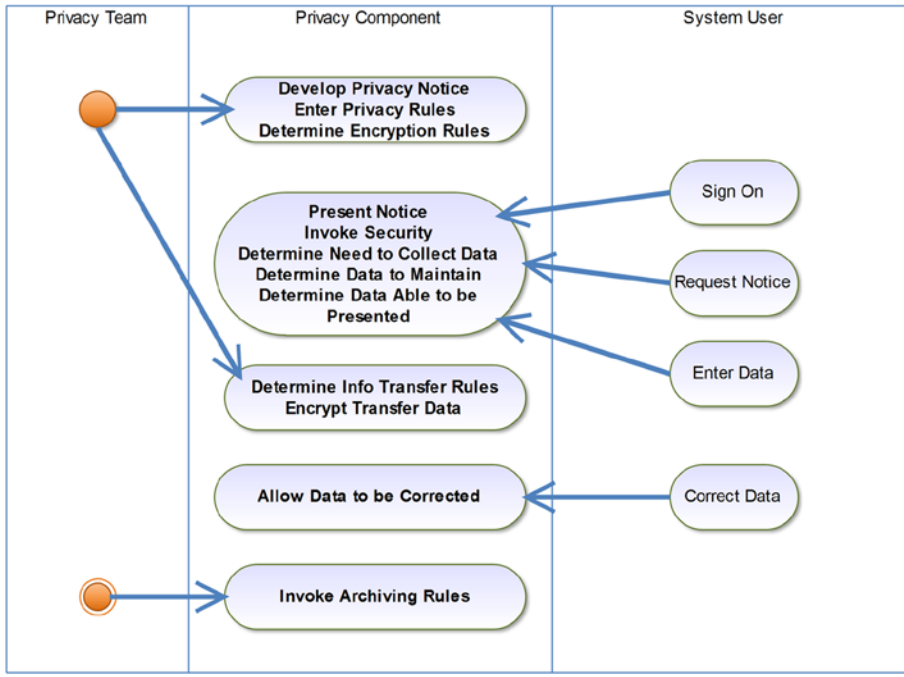



***Figure 7-5.*** *Privacy component system activity diagram*

Figure 7-5 shows that the privacy team begins the process by developing the Privacy Notice, developing and entering the privacy rules, and determining and causing implementation of the third-party transfer rules and the encryption mechanism. The system user uses the privacy component to make a Privacy Notice decision and to enter, maintain, and correct personal information according to privacy rules managed within the privacy component. The privacy component will periodically run the archiving rules under the direction of the privacy team.

## Privacy Assessment Using the System Activity Diagram

The system activity diagram is useful for documenting the design of the system. But just as important, the diagram can be used to assess how well the system satisfies the privacy principles' requirements. Figure 7-6 shows the system activity diagram with the FIPPS/GAPP principles designating which subcomponent satisfies each privacy principle. This assessment will also be useful as a tool for quality assurance and privacy impact assessment.

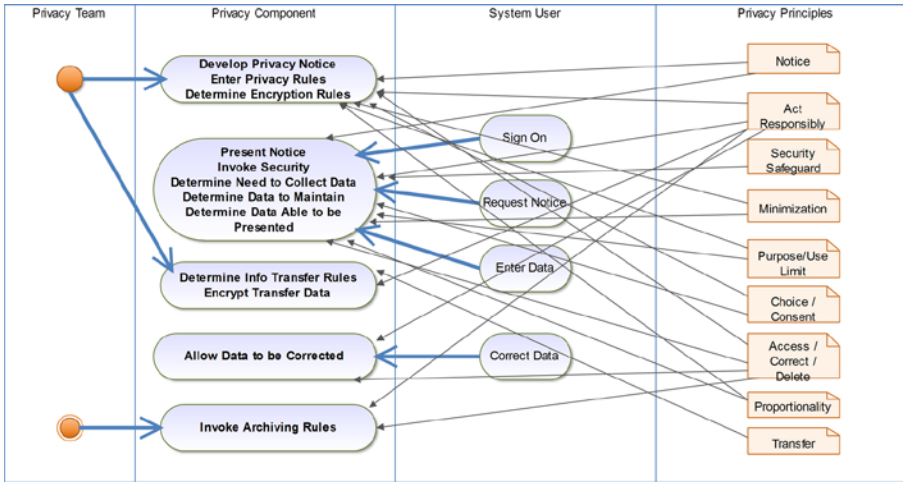



***Figure 7-6.*** *System activity diagram of the privacy component with a tie to privacy principles*

# Develop the Privacy Component Design

Figure 7-7 shows that the privacy component should have its own interface. The privacy component may be a web service whose user interface may be a web site. The embedding system often collects data and then passes the data through an API. These various data sources are passed through a well-known program pattern, the interface facade that allows data from the various sources to come into the component. The component may have a workflow manager that controls the privacy rules engine, a security subcomponent, and role data that are related to the privacy rules. The various transactions run by the privacy component will reach out to the various databases holding personal information and manage those data. Thus, the privacy component consists of a series of subcomponents and will be both data-centric and person-centric.

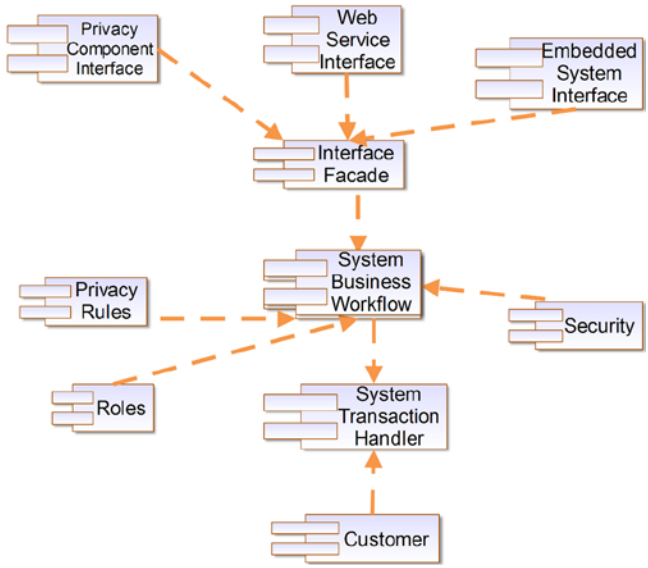



***Figure 7-7.*** *Component model for the privacy component*

# Using the System Development Methodology for the Privacy Component

A project to build a privacy component begins with project initiation. The privacy team and the system's engineering team who are knowledgeable in privacy engineering should first hold a short scoping workshop. The use case requirements should be developed along with the class and data modeling. Using both use case and the data model, the user interface will be designed. The development team will determine whether a user interface prototype will be necessary. A combination of the class model with the methods needed to support each class, the use case requirements, and the system activity diagram should be used to develop the component design and dynamic modeling sequence diagrams. From this documentation, the test cases are developed, including the system activity diagram showing the relationship of the privacy principles to the various subcomponents. Once the privacy component is developed and tested, an incremental rollout is recommended.

## INTUIT DATA STEWARDSHIP – AND DATA USE GUIDANCE – GIVING PRODUCT DEVELOPERS, MANAGERS AND DATA SCIENTISTS THE ABILITY TO IMPLEMENT ETHICAL PRIVACY DECISIONS.

By Barb Lawler

Chief Privacy Officer, Intuit

Data Stewardship Principles articulate a broad mission and guide product teams to use customer data to help customers improve their financial lives, while being clear that it is the customer's data, not ours. The principles were crafted less than three years ago with input from the highest levels of the company, including the CEO and a Co-founder. The principles define Intuit's role as a trusted steward of customers' data, specifically state that Intuit will give customers choices about Intuit's use of data that identifies them, and give open and clear explanations about how Intuit uses their data. Most importantly, the principles state that Intuit will not, without explicit permission, sell, publish or share entrusted customer data that identifies the customer or any person. Our customers have a basic expectation of privacy – but they have told us **they also expect us to find new ways to make their data to benefit them and help empower them** to improve their financial lives. There are dual consumer interests that need to be taken into account: consumer protection AND economic empowerment. At Intuit, we call this "Big Data for the Little Guy" – we give our small business customers the tools they have never had access to before, to harness the power of their data to deliver practical benefits for their business.

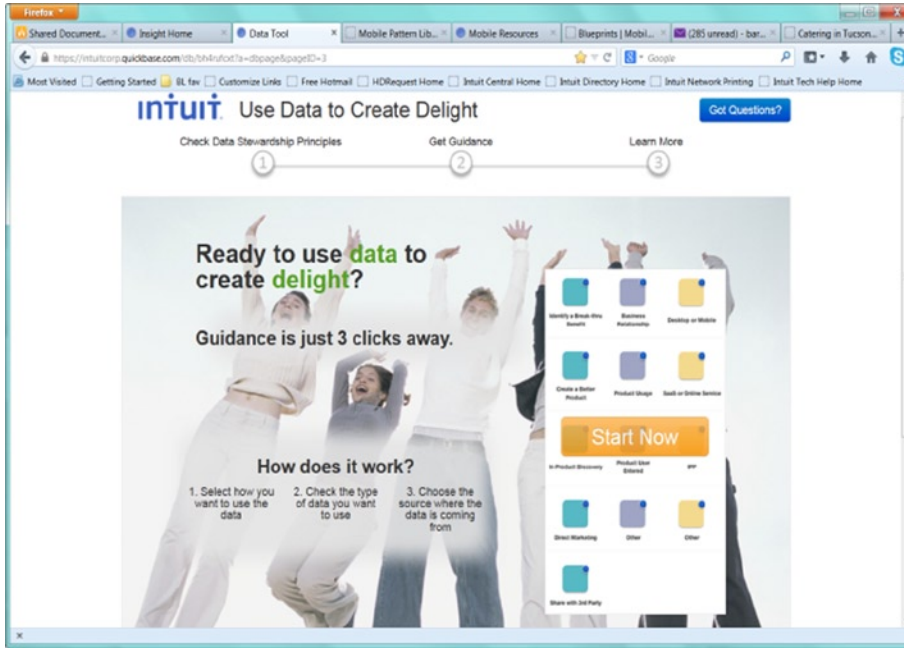
But how can the product manager, engineer or data scientists take action on these important concepts?

What if a product manager wants to use data to improve an offering or develop a cool new feature – can he do it, and if so how? Data scientists explore and test different theories to identify a breakthrough benefits and services, but they don't want to unintentionally misuse the customer data. Whatever the scenario, Intuit business unit and data services teams often have questions. Are they using the customer data in line with Intuit values, privacy policy and compliance requirements? Have other employees at Intuit used data in similar ways?

The Data Use Guidance Tool was developed to provide an interactive, automated tool developed to provide fast, consistent guidance for dozens of data use scenarios – taken from actual product usage, and to enable product teams to move quickly and with confidence. It also provides examples of best practices for informing and involving Intuit customers in the use of their data. Built using html on an Intuit QuickBase foundation, the Data Use Guidance tool is a rules-based engine drawing on no fewer than 500 "rules" behind the scenes. A group manager in analytics told us, "It makes gray, black and white. I know what my team can do with data."

The tool gives specific guidance to engineers in three easy steps. They select how they want to use customer data (e.g., direct marketing, share with a third party, etc.), check the type of data they want to use (e.g., business relationship, product usage, etc.) and choose the source of the data (e.g., desktop or mobile, SaaS or online service, etc.). Based on the selections made, the tool leads employees to one of three types of guidance: 1) Appropriate use – good to go; 2) Need to confirm and then go; and 3) Let's talk. At each step, the employees sees on-screen a summary of the steps he's taken. And with just one more click, he can navigate to a pattern library, with real examples of Intuit and external best practices for in-context transparency and choice. "Examples are so, so beneficial. I can develop and test quickly," commented a PM leader.

About half of all data use scenarios the tool will give developers the green light to move ahead without further consultation with the privacy team. At any time using the tool, they can request a consultation at the click of a button. This generates a confirmation e-mail, and the privacy team follows-up within one business day.



Example 1: A product manager would like to help a small business customer offer her employees a health benefit using a health payment card. Small Business owners have told us they want to be in control of the use of her employees' data and communication about the offer. The Tool guides the product manager to know that the customer would be involved and participate in the decision to share her employees' information with the third party delivering the Card. It shows the PM examples of how to describe the value and choice options to the Small Business owner and messaging to communicate to their employee about the offer within the product screen flows.

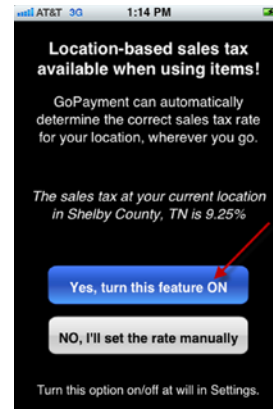
Example 2: A group marketing manager wants to conduct a direct marketing campaign that offers GoPayment, a mobile payment app and secure mobile device swiper to all QuickBooks Online customers using their business relationship data. The Tool shows the marketing pro that when he uses business relationship data to conduct this offer is an acceptable use of customer data which does not require additional action on his part (beyond applying relevant marketing preferences to the campaign mailing.

Example 3: A data scientist wants to evaluate a potential new business opportunity based on anonymous consumer financial transaction data from Mint and Quicken. The data scientist believes that this unique set of data, when combined with certain 3rd party data sets will create a unique perspective on consumer behavior which will be attractive in helping Small Business customers acquire new customers. The tool walks the data scientist through the type of use – a breakthrough benefit, the type of data – user entered in the products that is anonymized and 3rd party data. In this scenario, the Tool informs the data scientist that a consultation with the privacy team is required.

Example 4: Product developers use specific mobile privacy-by-design guidelines for smartphone and tablet applications. The Tool will take the mobile app developer directly to these guidelines, including mobile device patterns, which encourage the development and operation of mobile apps to reflect sound data privacy and protection policies that put customers first. The guidelines help developers understand:

- What data a mobile app may collect or access,
- How the data will be used and shared and for what purposes
- How the data will be stored and retained
- What choices the customer has over the collection and use of his/her data

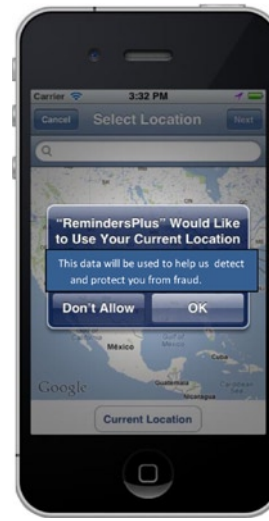
An example is how to effectively implement Geo-location. Customers will say 'yes' when the benefit is clearly stated and in context of the mobile applications operation and user flow.

| | | | |
|---|---|---|---|
| Geo-Location: Access, Collection & Use | We are transparent and provide choice if we access, collect, and use or store geo-location data. | Only access and/or collect geo-location data if it is required for the App's functionality and provides a clear benefit to the customer (e.g.,, facilitates local sales tax calculations or locates merchants).<br><br>**Collection.** To access and use geo-location data, we must notify the customer, describe how it will be used, and obtain customer consent before his or her geo-location data is accessed or used by our App.<br><br>• Notification and consent should be in real-time<br><br>• Consent should be affirmative, and not based on pre-checked boxes or preset defaults<br><br>• Notification should: alert customer to the collection of geo-location data, describe the purpose or benefit of the collection, and explain how the consent may be withdrawn (e.g., through a settings feature<br><br>• Customer should understand whether collection or use of geo-location data is a one-time event or ongoing (e.g., whether agreeing once to permit a geo-location feature causes this feature to remain on, until settings are adjusted) | **User Alerts.** Methods for alerting the customer to ongoing collection of geo-location data could include: (1) A symbol can be used to indicate an app is actively accessing and using geo-location to alert and give the customer access to geo-location data use and settings, or (2) A periodic email or push-notification can be sent reminding the customer that geo-location is enabled and how it may be disabled.<br><br>EXHIBIT B – Geo-Location<br>  |

(*continued*)

For Apple iOS, use the "Purpose" field to provide transparent notification of how the location data will be used.

**User Control.** If the geo-location consent is for ongoing use, and not a one-time use:




- Provide a means to alert the customer of the continued ongoing use of geo-location.
- If an application is closed, do not collect or use geo-location data unless the customer has specifically agreed to it.
- Provide easy to find and use settings that allow the customer to easily turn off geo-location tracking.

**Retention.** The retention period for geo-location data should be no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Unless there is a valid, approved business reason, geo-location data should be retained no longer than 24 hours unless it is anonymized.

Anonymized location data should not be re-identified, or maintained in a manner that allows for re-identification.

# Conclusion

This chapter discussed the privacy component, which is a unique aspect of this privacy engineering approach. It allows the privacy rules based on privacy policies to be added and maintained in one place. It can be used as a standalone application or as a web service. As a standalone app, the Privacy Notice can be maintained and privacy rules can be entered and maintained. When the privacy component is embedded in a system or app, the database designed from the privacy component data model may be maintained in whole or in part within the privacy component portion of the system. The key business purpose of the privacy component is to ensure that the required privacy policies are enforced in a uniform manner. Chapters 8 and 9 will discuss applications where the privacy component may be used.

The sidebar discusses a wonderful program that developed in parallel to the writing of this book. It provides a practical example of a rule-based program and a proof of the privacy component concept.