



---

Privacy by Design

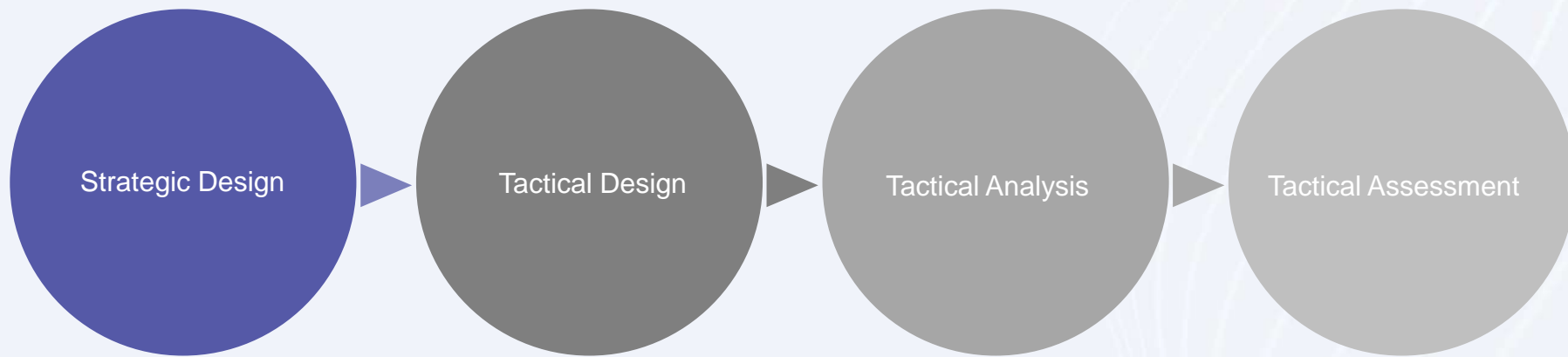
# Analysis Report

August 2021

PREPARED BY:

**ENTERPRIVACY**  
CONSULTING GROUP

This is  
**Level 1 Strategic Design**  
Analysis



---

**Level 1**  
Strategic Design

Based on the goals and quality attributes of the product, service or process being reviewed, a strategic design report identifies individuals at risk, threat actors, information and qualifies the factors contributing to privacy risk. It concludes by identifying strategies to mitigate those risks and where those strategies ought to be applied.

---

**Level 2**  
Strategic Gaps  
and Tactical Design

A tactical design report expands on the strategic design report by identifying strategic gaps between the proffered design and the architecture of the actual product, service or process. For non-deployed strategies, this report indicates the organization's justification and analysis as to why the strategy was not used. For deployed strategies, the report details tactical design recommendations for each strategy.

---

**Level 3**  
Tactical Analysis

A tactical analysis report identifies gaps between the proposed tactics in the tactical design report and implemented tactics. It analyzes whether other employed tactics sufficiently mitigate risks.

---

**Level 4**  
Tactical Assessment

A tactical assessment looks at a range of identified tactics implemented by the organization and reviews the sufficiency of the implementation to mitigate risks. Unlike the other reports, this is limited in scope to a predefined set of tactics desiring extra scrutiny.

# Table of Contents

Executive Summary 04

Description 05

Individuals At Risk 06

Threat Actors 07

Threat Landscape Diagrams 08

Mitigation Opportunities 15

Design Strategies 17

## Executive Summary

Enterprivacy Consulting Group (“Enterprivacy”) reviewed the digital assistant company, Wellbeity, a scheduling automation and payment service for psychotherapists and their clients. This level one strategic privacy design analysis includes a contextual landscape of Wellbeity’s service, a high-level risk analysis and opportunities for risk mitigation.

*In addition to the two at-risk individuals, Enterprivacy identified two goals of the service, five quality attributes that could affect individual privacy, 13 potential threat actors and around 150 opportunities for strategic reduction of privacy risks.*

Importantly the risks associated with every other threat actor can be reduced by choices made by Wellbeity in the design and architecture of their system. Mitigation opportunities are shown at the end of this report and those opportunities should provide a starting point for Wellbeity to explore specific tactical implementations to reduce risks to clients and therapists alike.

### KEY FINDINGS

1. Acquaintances of therapists’ clients pose a significant risk to clients. Acquaintances may have access to client email or calendars and may have access to information contained in those emails or calendar invites which disclose sensitive information about the type or nature of the session the client has scheduled. This may also lead to more tangible consequences in the relationships between clients and acquaintances.
2. Given the reliance on third party tools (calendars, email systems, video systems, etc.) and the power difference between Wellbeity as a startup and these established vendors, Wellbeity is not in a position to dictate (or supervise) the controls in place by these vendors. It would be well advised that Wellbeity should sufficiently warn therapists of the risks, support and choose vendors with a pro-privacy stance, and institute control within its control, such as limiting the information shared with these vendors.

Disclaimer: This analysis is based on public information and information provided by the company on the nature of the provided services. In the event there are system components or functionality that was not identified, this analysis would not cover those risks or possible mitigation strategies. In addition, the risk factors and suggested controls are based on educated guesses and broad categorizations of the threat actors, threats and appropriateness and adequacy of potential controls.

# Description

Wellbeity is a service designed to assist psychotherapists in managing client engagements. Therapists can describe types of services offered and show available session dates and times. Clients can select, book and initiate payments for appointments through an interface (i.e. widget) on the therapists' website. Clients refer to the therapists clients or potential clients. Appointments bookings will be submitted to both therapist and client calendars via email.



Two primary goals for the service were discerned from our discussion and investigation into the Wellbeity service:

**Goal 1 (G1) to help therapists manage client engagements (bookings and payments)**

**Goal 2 (G2) to help clients simplify booking process with therapists**

In addition, Enterprivacy identified a nonexhaustive list of quality attributes likely to be required of the service. Quality attributes, sometime called non-functional requirements, are qualitative properties the service should exhibit.

- Q1** Accessibility
- Q2** Administrability
- Q3** Interoperability - with therapist websites, video providers and calendar provider
- Q4** Reliability
- Q5** Supportability
- Q6** Securability
- Q7** Simplicity
- Q8** Usability

# Individuals At-Risk

In reviewing the service offering, Enterprivacy found two categories of individuals at risk of potential privacy issues by the Wellbeity service: therapists (who are Wellbeity's customers) and clients of therapists. While there were other potential at risk individuals, we choose to focus our analysis on these two.

## first-party consumers:

*The individuals receiving the results of the product, service or business process (commonly consumers but could be employees if the service is provided to employees)*

**A**

**Client** - Clients benefit from the automation of the booking process, which simplifies the process, and saves their time and effort to find and book a session.

**B**

**Therapist** - Therapists benefit from automation of the bookings and payments, which saves their time and resources making them more efficient.

## first-party providers:

*The individuals involved in providing the product, service or business process (commonly employees or contractors)*

This analysis did not review the affects on Wellbeity employees or others involved in providing the service.

# Actors

The table below identifies the actors most likely to pose a problem to the privacy of clients or therapists in the Wellbeity system. The list is non-exhaustive but represents, in Enterprivacy's opinion, the actors that are most relevant. Other potential actors include the network providers but these are excluded because not much they will do or can be done about them. However, they need to be considered for security purposes separate from the privacy risks identified in this analysis.. Also this analysis excluded "Acquaintance of the Therapists" who may glean information from the Therapists' calendar or email. Hopefully, therapists will take reasonable precautions to avoid non-professional access to their professional information.

#	Actor	Type	Motives	Resource Level
1	Wellbeity			Small to medium
2	Wellbeity Team			Amateur
3	Video Provider			Medium to large
4	Calendar Provider			Medium to large
5	Email Provider			Medium to large
6	Cyber-Criminal			Amateur to Professional
7	Payment Provider			Medium to large
8	Third Party Services (like CRM, Slack, or other vendor services)			Small, medium or large
9	Social Media Provider			FAAMG
10	Clients			Amateur
11	Therapists			Amateur
12	Therapists website operators (developer/host)			Small, medium or large
13	Acquaintance (of client)			Amateur

**Type:** Organization Person **Motives:** Money Competitive Advantage Revenge Spite Curiosity Control

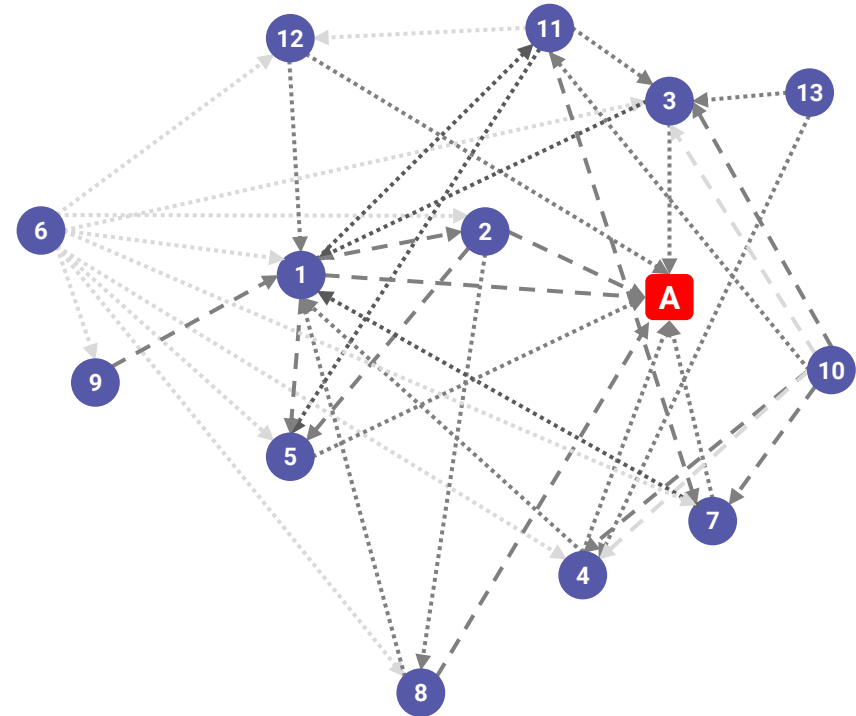
# Threat Landscape Diagrams - Clients

The following diagram illustrates the interactions between actors or between an actor and a proxy for the individual at-risk. Proxies, or stand-ins, represent the at-risk individual and include information about the individual, property of the individual or friends and family of the individual.

## LEGEND:

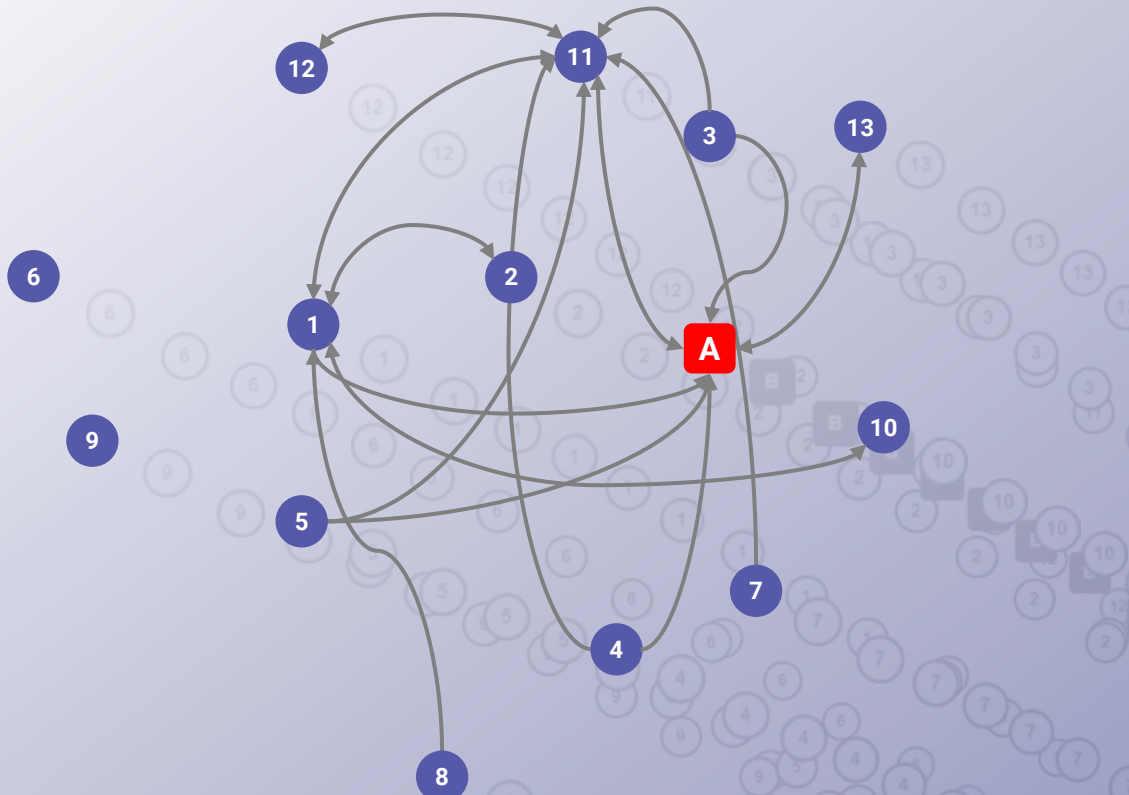
Interactions:	
Straight Line —————>	mean interactions between the actor and an at-risk individual, possible through another actor.
Dotted Line .....>	means it's not a direct interaction, but through a proxy (information, property or friends and family of the individual).
Dashed Line - - - ->	means actor interacts with at-risk individual, directly and through a proxy.

- Wellbeity (1) interacts with [A](both directly and via a proxy), 1 also interacts with [A] through email provider (5)
- Wellbeity Team (2) interacts with [A] (both directly and via a proxy), it also interacts with B through email provider (5), through Wellbeity's systems (1) and through Third Party Services (8)
- Video Provider (3) interacts with [A]'s proxy (information and/or device), and interacts with [A]'s data through 1 (Wellbeity's systems)
- Calendar Provider (4) interacts with [A]'s proxy (information and/or device) either directly or through 1(Wellbeity's systems)
- Email Provider (5) interacts with [A]'s proxy (information and/or device)
- Payment Provider (7) interacts with [A]'s proxy (information and/or device) either directly or through 1(Wellbeity's systems)
- Third Party Services (8) interact with [A] (both directly and via a proxy), 8 also interacts with [A]'s data through Wellbeity's systems (1)
- Social media provider (9) interacts with [A]'s data through (1)'s systems
- Clients (10) interacts with [A] (directly and via a proxy) through the video provider (3), and through calendar provider (4)  
Could be on purpose (like group sessions) or through a leak with bad URLs
- Therapists (11) interact with [A] and [A]'s proxy through Wellbeity (1), through email provider (5) and through video provider (3)
- Therapists' websites (12) interacts with [A] through a proxy, and also interacts with [A] through Wellbeity (1)
- Acquaintance (13) interacts with [A] and [A]'s data through Video provider or interacts with [A]'s data though calendar provider



**Interactions** diagram for client (at-risk individual A)

# Threat Landscape Diagrams - Clients

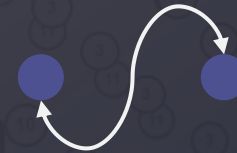


**Relationships** diagram for clients (at-risk individual A):

## LEGEND:

A curved line indicates a relationship between actors; for instance, employer/employee or contractual relationship.

Arrows on curved connectors:



X and Y have a bidirectional relationship (e.g. contract with equal power in negotiations)



X and Y have no relationship



X and Y have one directional relationship where X has power over Y (e.g. employer/employee)

The diagram above illustrates the relationships between actors. Relationships can pinpoint disparities in power that may heighten risks from a threat actor to an individual or it can suggest opportunities for supervision of threat actors.

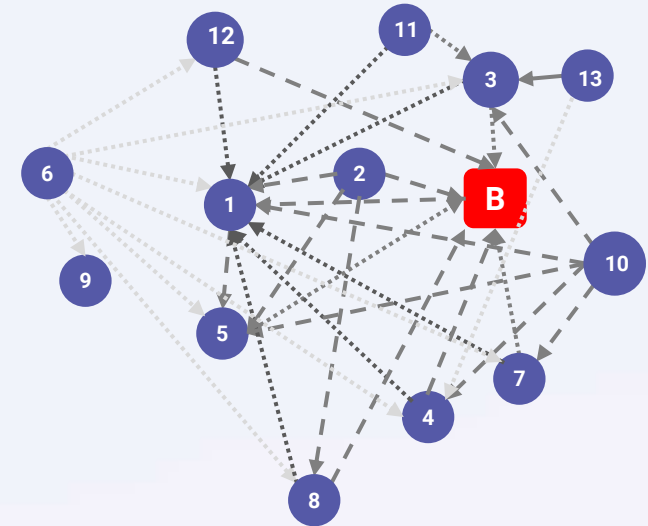


# Threat Landscape Diagrams - Therapists

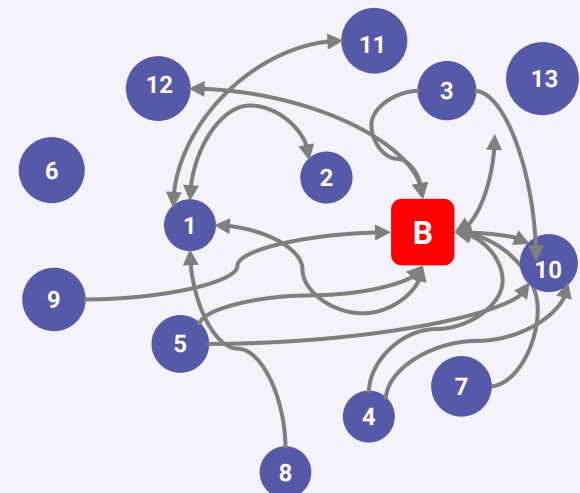
The following diagram illustrates the interactions between actors or between an actor and a proxy for the individual at-risk. Proxies, or stand-ins, represent the at-risk individual and include information about the individual, property of the individual or friends and family of the individual.

- Wellbeity (1) interacts with [B] (both directly and via a proxy),
- (1) also interacts with [B] through email provider (5)
- Wellbeity Team (2) interacts with [B] (both directly and via a proxy), through email provider (5), through Wellbeity's systems (1) and through Third Party Services (8)
- Video Provider (3) interacts with [B]'s proxy (information and/or device), and interacts with [B]'s data through 1 (Wellbeity's systems)
- Calendar Provider (4) interacts with [B]'s proxy (information and/or device) either directly or through (1)(Wellbeity's systems)
- Email Provider (5) interacts with [B]'s proxy (information and/or device)
- Payment Provider (7) interacts with [B]'s proxy (information and/or device) either directly or through (1) (Wellbeity's systems)
- Third Party Services (8) interact with [B] (both directly and via a proxy), 8 also interacts with [B]'s data through Wellbeity's systems (1)
- Social media provider (9) interacts with [B]'s data through (1)'s systems
- Clients (10) interacts with [B] through the video provider (3), through email provider (5), through wellbeity's systems (1) and through calendar provider (4)
- Other Therapists (11) interact with [B]'s data through Wellbeity and through [B]'s website (12)
- Therapists website (12) interacts with [B] both directly and through a proxy, and also interacts with [B] through wellbeity (1)
- Acquaintance (13) interacts with [B] through Video provider or interacts with [B]'s data through calendar provider

**Interactions** diagram for therapists (at-risk individual B)



**Relationships** diagram for therapist (at-risk individual B)



The diagram at right illustrates the relationships between actors. Relationships can pinpoint disparities in power that may heighten risks from a threat actor to an individual or it can suggest opportunities for supervision of threat actors.

# Risk Factors for Each Harm - Clients

For each threat the following factors are considered.

O = Opportunity of the threat actor (every line on the interactions diagram presents opportunity)

M = Motivation by the threat actor

S = Severity or non-normativity of this activity

C = Consequences (Tangible) based on sensitivity of the at-risk individual

Interactions with information as the proxy present opportunities Information Processing and Information Dissemination harms. Direct interactions, or those towards a proxy, present an opportunity for Collection and Invasion harms. Motivation, severity and consequences are marked if they are non-negligible. Yellow highlights indicate presence of all four factors. Lavendar highlights indicate presence of at least three factors.



Yellow indicates all factors present



Lavender is at least three factors

Potential Harms for clients from	Threat Actor												
INFORMATION PROCESSING	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Aggregation</b> combining of various pieces of personal information	OMC	OSC	OM	OM	OM	OMS	OM	OM	OMC	OS	OMSC	OSC	OMSC
<b>Identification</b> linking of information to a particular individual	OM	OSC	OM	OM	O	OMS	OM	OM	OMC	OMSC	OMSC	OS	OMSC
<b>Insecurity</b> carelessness in protecting information from leaks or improper access	OC	OSC	OMSC	OMSC	OMSC	OMS	OMSC	OMSC	OMC	OS	OMSC	OMSC	
<b>Secondary Use</b> using personal information for a purpose other than the purpose for which is was collected	OS	OSC	OM	OM	OM	OMSC	OMS	OM	OMC	OSC	OMSC	OMSC	OMSC
<b>Exclusion</b> failing to let an individual know about the data that others have about them and participate in its handling or use	OS	OSC	OM	OM	OM	OMS	OM	OM	OMC	OS	OMSC	OSC	OMSC

INFORMATION DISSEMINATION	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Breach of Confidentiality</b> breaking a promise to keep a person's information confidential	OSC	OSC	OMSC	OMSC	OSC	M	OMSC	OMSC	OMSC	OSC	OSC	OSC	OMSC
<b>Disclosure</b> revealing truthful personal information about a person that impacts the ways others judge their character or impacts their security	OSC	OSC	OSC	OSC	OSC	OMSC	OSC	OSC	OSC	OSC	OSC	OSC	OMSC
<b>Exposure</b> revealing an individual's nudity, grief, or bodily functions	SC	SC	OSC	SC	OSC	OMS		OS	OS	SC	SC	OSC	OMSC
<b>Increased Accessibility</b> amplifying the accessibility of personal information	OMS	OSC	OSC	OSC	OSC	OMSC	OSC	OSC	OMSC	OSC	OSC	OSC	OMSC
<b>Appropriation</b> using an individual's identity to serve the aims and interests of another	OMS	OSC	OSC	OSC	OSC	OMS	OS	OSC	OMSC	OSC	OSC	OSC	
<b>Distortion</b> disseminating false or misleading information about an individual	OSC	OSC	OSC	OSC	OSC	OMSC	OSC	OSC	OS	OSC	OSC	OSC	OMS
COLLECTION	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Surveillance</b> watching, listening to, or monitoring of an individual's activities	OSC	OSC	O	O	OM	MSC	OM	OMS	OM	OSC	OMSC	OMS	OMSC
<b>Interrogation</b> questioning or probing for personal information	OMS*	OSC	O	OM	O	MSC	OM	OMS	OM	OMSC	OMSC	OMSC	OMSC
INVASION	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Intrusion</b> disturbing an individual's tranquility or solitude	OS*	OSC	OSC	OSC	OSC	MSC	S	OSC	OMC	OMSC	OMSC	OSC	OMSC
<b>Decisional Interference</b> intruding into an individual's decision regarding their private affairs	OMSC	OSC	OC	OMC	OC	MSC	OMSC	C	OMC	OSC	OMSC	OMSC	OMSC

# Risk Factors for Each Harm - Therapists

Potential Harms for therapists	Threat Actor												
INFORMATION PROCESSING	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Aggregation</b> combining of various pieces of personal information	OMC	OS	OM	OM	OM	OMS	OM	OM	OM	OMC	OMC	0	
<b>Identification</b> linking of information to a particular individual	OM	OS	OM	OM	0	OMS	OM	OM	OM	OM	OMC	0	
<b>Insecurity</b> carelessness in protecting information from leaks or improper access	OC	OSC	OMSC	OMS	OMS	OMS	OMSC	OMSC	OM	0	0	OMSC	
<b>Secondary Use</b> using personal information for a purpose other than the purpose for which is was collected	OS	OSC	OM	OM	OM	OMSC	OMS	OM	OMC	OC	OMC	0	
<b>Exclusion</b> failing to let an individual know about the data that others have about them and participate in its handling or use	OS	OS	OM	OM	OM	OMS	OM	OM	OMC	OC	OMC	0	
INFORMATION DISSEMINATION	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Breach of Confidentiality</b> breaking a promise to keep a person's information confidential	OSC	OS	OMSC	OMSC	OSC		OMSC	OMS	OMSC	OS		OSC	
<b>Disclosure</b> revealing truthful personal information about a person that impacts the ways others judge their character or impacts their security	OSC	OSC	OSC	OSC	OSC	OMSC	OSC	OS	OS	OMSC	OMSC	OC	
<b>Exposure</b> revealing an individual's nudity, grief, or bodily functions	SC		OS										
<b>Increased Accessibility</b> amplifying the accessibility of personal information	OMS	OS	OSC	OSC	OSC	OMSC	OSC	OS	OMC	0	OC	OC	
<b>Appropriation</b> using an individual's identity to serve the aims and interests of another	OMS	OS	OSC	OSC	OSC	OMSC	OS	OS	OMS	0	OMSC	OM	
<b>Distortion</b> disseminating false or misleading information about an individual	OSC	OSC	OSC	OSC	OSC	OMSC	OSC	OS	OSC	OMSC	OMSC	OC	

COLLECTION	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Surveillance</b> watching, listening to, or monitoring of an individual's activities	OSC	OS	0	0	OM	MS	OM	OMS	OM	OSC	0	0	
<b>Interrogation</b> questioning or probing for personal information	OMS*	OS	OM	OM	0	MS	OM	OMS	OMC	OMSC	0	0	
INVASION	1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Intrusion</b> disturbing an individual's tranquility or solitude	OS*	OSC	OSC	OSC	OSC	MSC		OSC	OMC	OMSC	OC	OM	
<b>Decisional Interference</b> intruding into an individual's decision regarding their private affairs	OMSC	OS	OMC	OMC	OC	MSC	OMSC		OMC	OSC	OSC	OMC	



# Mitigation Opportunies

Wellbeity is in a position to mitigate threats posed by each of the other threat actors through several architectural strategies of minimizing and seperating threat actors from people or information where practical, securing information by hiding or abstracting it, and balancing information and power asymmetiries by informing therapists and their clients and giving them opportunity to control interactions. For instance, Wellbeity could minimize the data in the calendar invite, requiring login by clients to get information on the session (who it is with, where, etc..)

Also, isolating the data to those that have access to their platform would reduce risks posed by cilent acquaintences to therapists' clients. Descriptions of the strategies and underlying tactics are available in the next section.

Because of it's strategic placement, Wellbeity can apply various design strategies (Achitect, Secure and Balance to mitigate riskposed by each of the threat actors

①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
👤🔒📅	👤🔒📅👥		👤🔒📅	👤🔒📅	👤🔒📅	👤🔒📅	👤🔒📅	👤🔒📅	👤🔒📅👥	👤🔒📅👥	👤🔒📅	👤🔒📅

Deleting data after use to prevent future Wellbeity from using it for a secondary purpose

Encrypt data in the Wellbeity systems

See Next Page

Minimize the data in the calendar invite, requiring login by clients to get information on the session (who it's with, where, etc..)

Wellbity can also supervise the activities of it's founders,

② Wellbeity Founders

①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
👤🔒📅👥	👤🔒📅👥	📅	📅	👤🔒📅	👤🔒📅	📅	👤🔒📅	📅	📅	📅	📅	📅


Wellbeity (continued from previous page)

⑩

⑪




?

?

Wellbeity can supervise  the clients...

and the therapist through term of service and contract terms

⑩ Clients

①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
												

⑪ Therapist

①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
												

Therapists can supervise their websites

⑫ Therapists Websites

①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
												

# TECHNICAL STRATEGIES



ARCHITECT



SECURE



MINIMIZE

► **Exclude**

Limit interactions and information to only that which is necessary to complete the task

► **Select**

Limit interactions and information on a case by case basis

► **Strip**

Limit interactions and information on a case by case basis

► **Destroy**

Remove information after processing



SEPARATE

► **Isolate**

Limit interactions and information to only that which is necessary to complete the task

► **Distribute**

Physically separate interactions or information



ABSTRACT

► **Group**

Aggregate information about groups of individuals

► **Summarize**

Generalize detailed information into less granular attributes

► **Perturb**

Add noise or approximate the real value of data



HIDE

► **Restrict**

Prevent access to persons or information them

► **Mix**

Randomize people or Information about them to remove correlations

► **Obfuscate**

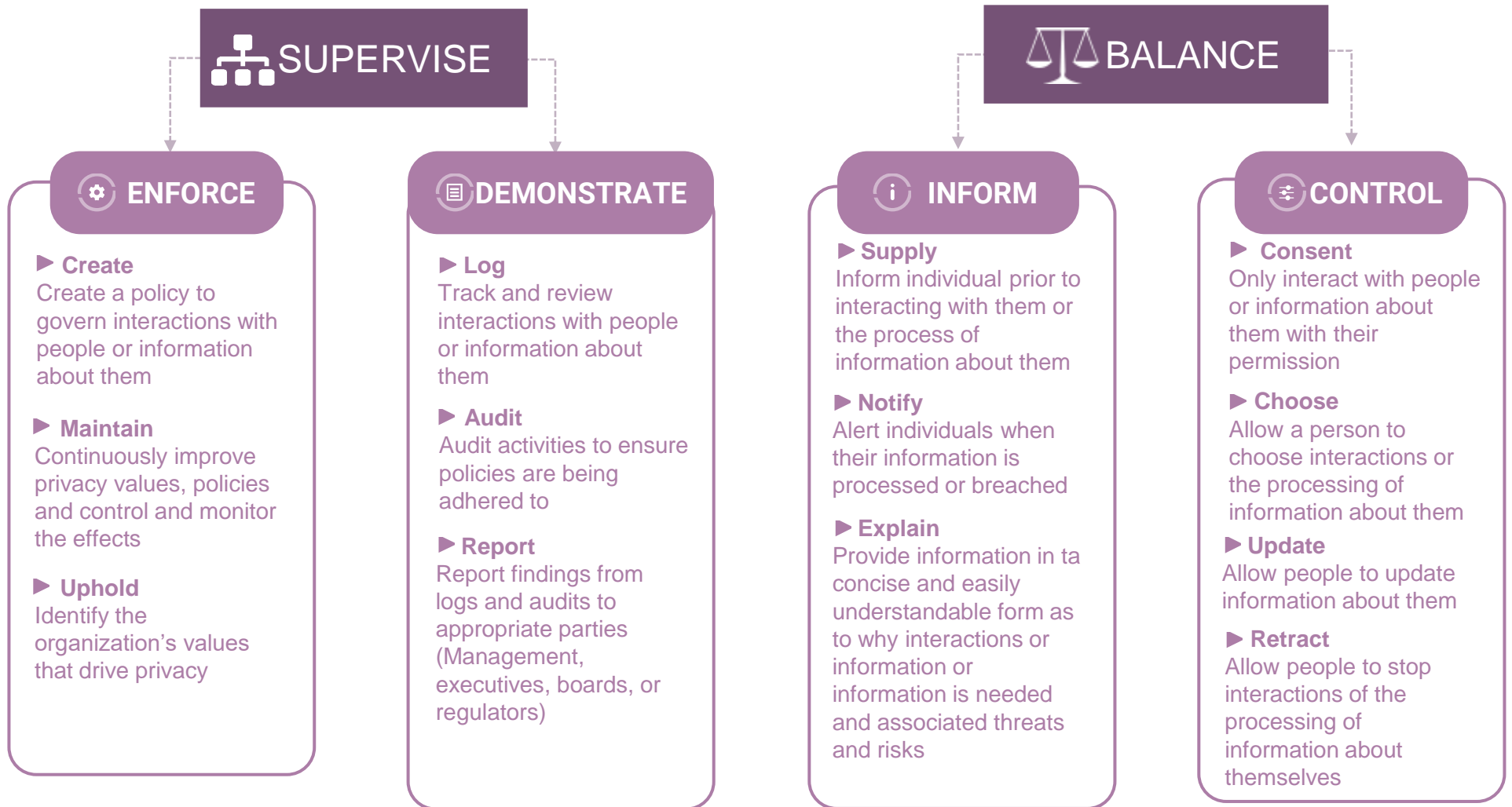
Reduce correlations between people or a person and information about them

► **Dissociate**

Remove correlations between people or a person and information about them



# PROCESS STRATEGIES





**ENTERPRIVACY**  
CONSULTING GROUP