

The Respect Trust Framework™

PUBLIC REVIEW DRAFT #1 PUBLISHED 2011-05-10

Single Page Summary

Purpose

The purpose of the Respect Trust Framework is to define a simple set of principles and rules to which all Members of a digital trust network agree so that they may then share identity and personal data with a higher degree of confidence that it will be safe and only used as authorized.

Principles

Principle	Synopsis	Wording
Promise	<i>We will respect each other's digital boundaries</i>	Every Member promises to respect the right of every other Member to control the identity and personal data they share within the network and the communications they receive within the network.
Permission	<i>We will negotiate with each other in good faith</i>	As part of this promise, every Member agrees that all sharing of identity and personal data and sending of communications will be by permission, and to be honest and direct about the purpose(s) for which permission is sought.
Protection	<i>We will protect the identity and data entrusted to us</i>	As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of identity and personal data shared with that Member.
Portability	<i>We will support other Members' freedom of movement</i>	As part of this promise, every Member agrees to ensure the portability of the identity and personal data shared with that Member.
Proof	<i>We will reasonably cooperate for the good of all Members</i>	As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.

Rules

The Respect Trust Framework is made self-reinforcing through use of a peer-to-peer reputation system consisting of two parts: the *Respect Vouching System* for positive reputation and the *Respect Conflict Resolution System* for negative reputation. Both are defined in this document.

The Respect Promise™

The Respect Promise is the contractual commitment made by and among Members upon joining the trust network that establishes mutual duties and benefits among all Members as expressed by the statement: "I promise to uphold the purposes and principles of the Respect Trust Framework."

Table of Contents

SINGLE PAGE SUMMARY	1
PURPOSE	1
PRINCIPLES	1
RULES	1
THE RESPECT PROMISE™	1
TABLE OF CONTENTS	2
STATUS: PUBLIC REVIEW DRAFT #1	3
PURPOSE	4
PRINCIPLES	4
THE FIRST PRINCIPLE: PROMISE	5
THE SECOND PRINCIPLE: PERMISSION	6
THE THIRD PRINCIPLE: PROTECTION	6
THE FOURTH PRINCIPLE: PORTABILITY	7
THE FIFTH PRINCIPLE: PROOF	7
VERSIONING AND AMENDMENTS	8
PLUG-IN TRUST FRAMEWORKS	8
COPYRIGHTS AND TRADEMARKS	9
EXHIBIT A: THE RESPECT VOUCHING SYSTEM	10
DEFINITIONS	10
GENERAL RULES FOR VOUCHING	10
SPECIFIC RULES FOR TRUST ANCHOR VOUCHING	11
SPECIAL RULES FOR FOUNDING TRUST ANCHORS	11
EXHIBIT B: THE RESPECT CONFLICT RESOLUTION SYSTEM	12
EXHIBIT C: COMPARISON OF THE RESPECT PRINCIPLES AND FIPPS	22

Status: Public Review Draft #1

This draft of the Respect Trust Framework was submitted by [Connect.Me](#) on 10 May 2011 for publication with the Open Identity Exchange (OIX)¹ as a digital trust framework in accordance with the [Open Identity Trust Framework Model](#).² As the name implies, OIX is an open exchange on which trust frameworks are listed for public inspection and usage by different market participants. The Respect Trust Framework was specifically developed to address the market need to increase the level of control that all legal persons (both individuals and organizations) have over their digital identity and personal data.

Because the Respect Trust Framework will serve as the Member contract for the Connect.Me digital trust network, Connect.Me and the [Personal Data Ecosystem Consortium](#) (PDEC)³ are providing a public review period of at least 30 days prior to the formal launch of the Connect.Me Network.

Connect.Me and PDEC invite your feedback and input by participating in the Respect Trust Framework Discussion Forum. Details of this forum, hosted by PDEC, are available at the PDEC home page at <http://personaldataecosystem.org/>.

As feedback is reviewed, comments and suggestions that are consistent with the Respect Trust Framework's purpose, principles, and administration will be incorporated into one or more subsequent public review drafts, each of which will be submitted by Connect.Me for publication by OIX. Each new public review draft will be announced on the Respect Trust Framework Discussion Forum and also on the Connect.Me blog at <http://blog.connect.me>, and Twitter feed at [@respectconnect](#).

Connect.Me serves as the provider of the Connect.Me Network, which incorporates the Respect Trust Framework into its Member contract. Connect.Me has discretion and authority to decide upon the Connect.Me Terms of Service, Rules, and Privacy Policy (collectively the Connect.Me Terms) which are separate from the Respect Trust Framework. However Connect.Me as the network provider is subject to the Respect Trust Framework in the same way as every other Member, so the Connect.Me Terms must be entirely consistent with the Respect Trust Framework. Members exercise their authority regarding the Connect.Me Terms when they determine whether or not to join the Connect.Me Network in its final form following the public review period.

Once the first version of the Respect Trust Framework is finalized and is accepted as part of the Member contract for Members of the Connect.Me Network, further revisions require a vote of qualified members as defined in the Versioning and Amendments section of this document. This ensures that future evolution of the Respect Trust Framework happens only with the input and consent of the Members.

¹ <http://www.openidentityexchange.org/>

² <http://www.openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf>

³ <http://personaldataecosystem.org/>

Purpose

The purpose of the Respect Trust Framework is to define a simple set of principles and rules to which all Members of a digital trust network agree so that they may then share identity and personal data with a higher degree of confidence that it will be safe and only used as authorized.

Principles

Following are the five fundamental principles upon which the Respect Trust Framework is based:

Principle	Synopsis	Wording
Promise	<i>We will respect each other's digital boundaries</i>	Every Member promises to respect the right of every other Member to control the identity and personal data they share within the network and the communications they receive within the network.
Permission	<i>We will negotiate with each other</i>	As part of this promise, every Member agrees that all sharing of identity and personal data and sending of communications will be by permission, and to be honest and direct about the purpose(s) for which permission is sought.
Protection	<i>We will protect the identity and data entrusted to us</i>	As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of identity and personal data shared with that Member.
Portability	<i>We will support each other Member's freedom of movement</i>	As part of this promise, every Member agrees to ensure the portability of the identity and personal data shared with that Member.
Proof	<i>We will reasonably cooperate for the good of all Members</i>	As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.

These principles, called the Respect Principles or just Principles, were extracted from the common elements of privacy, data protection, and trust across different jurisdictions and legal traditions around the world. Exhibit C provides a chart that matches the principles with different versions of Fair Information Practices Principles (FIPPs) from different countries and international organizations, as well as with common law principles.

The following sections provide further guidance to understanding and interpreting each Principle, including examples of the “duties of care” for handling of identity and personal data consistent with each principle. The guidance below is intended to be normative, i.e., it is intended to be relied upon directly in the application and interpretation of the Respect Trust Framework. The examples provided are intended for illustrative purposes only.

Like the examples, Exhibit C sets forth additional guidance for application of the Principles that is intended to be merely “informative,” not normative. In the case of Exhibit C, it is recognized that authority for existing FIPPs may vary from one legal jurisdiction to another. The chart in Exhibit C illustrates specifically how the Principles relate to current legal authorities. More generally, the individual FIPPs associated with each Principle provide examples of the types of specific duties that are intended to be covered by each Principle, and thereby they collectively help to inform how the Principles may be interpreted.

Notably, most FIPPs were developed to cover the needs of only individual data subjects (primarily in the context of data collections by governmental and commercial parties). The Respect Principles are broader, intending to support the integrity of all data subjects, whether individual, commercial, governmental, or otherwise. As a result, existing FIPPs should be consulted with the understanding that they need to be broadened to cover all entities, not just individuals.

The First Principle: Promise

***Promise.** Every Member promises and agrees to respect the right of every other Member to control the identity and data they share within the network and the communications they receive within the network.*

The first Principle represents each Member’s agreement to be bound by the duty to respect each other Member’s online “identity integrity” in all circumstances, even without being asked by another Member to do so.

Without the respect by outside parties of a person’s “boundaries,” their identity has uncertain integrity, which is perceived by an individual person as a lack of privacy and security, and by a legal entity as a lack of security and increased liability risk. Just as people and entities in the physical world need protection from “trespass,” “unreasonable searches and seizures,” unauthorized access, and other physical and perceptual intrusions, individuals and legal entities need to be able to maintain identity integrity against similar intrusions online.

This Principle is directed at causing Members to adopt the duties, in their role as data handlers, to respect other Member’s online identity integrity. The duties are directed toward data flows in two directions. Identity integrity is proportional to the degree to which a data subject has control of both their inputs (what data and communications they receive) and outputs (how data about them and information about them observed by others is distributed). Both are covered in the Promise Principle.

The common law privacy tort of “unreasonable intrusion upon another’s seclusion” is a traditional root of this principle. Not all international jurisdictions embrace that particular concept in law, but each has some concept of the legal boundaries that separate one legal entity from another. By making the promise in the Promise Principle, each Member is simply stating that they will respect those legal boundaries, consistent with local customs, local law, and the Respect Trust Framework. A breach of duty under the Promise Principle to respect identity generally constitutes an intrusion. For example, intrusions include those legally cognizable as torts, crimes, and civil rights violations.

Another way to view this Principle is as an instantiation in digital terms of the ethic of reciprocity widely known as “The Golden Rule.” In essence, the first Principle is the duty of each Member to “*treat data about others as you would like them to treat data about you*”.

So fundamental is this principle to the Respect Trust Framework that the other four principles are all stated as extensions to this principle.

In addition, this principle also represents the contractual commitment all Members are making to other Members when they join a trust network such as the Connect.Me Network operating under the Respect Trust Framework. For this reason it is referred to with the trademarked **The Respect Promise™**. This is explicitly defined to mean:

“I promise to uphold the purpose and principles of the Respect Trust Framework.”

The Second Principle: Permission

Permission. *As part of this promise, every Member agrees that all sharing of identity and personal data and sending of communications will be by permission, and to be honest and direct about the purpose(s) for which permission is sought.*

The second Principle clarifies that one specific aspect of each Member’s duty to respect the integrity of each other Member’s digital boundaries is by seeking permission to “cross” them, i.e., to specifically request consent from another Member to use shared data or to send communications, and to do so with an honest and clear statement of the purposes of the request.

While the first Principle sets up a default duty of non-intrusion (aka respect for identity integrity), the second Principle anticipates that what would otherwise be an “intrusion” may be authorized with “permission” when that permission is fairly and reasonably sought.

Examples of harms resulting from violation of this second Principle in the physical world are characterized as the traditional torts and legal “causes of action” referred to as “infringement,” “conversion,” “misappropriation,” “violation of publicity rights,” and “unjust enrichment.” All of these involve harms to a person from use of or intrusion upon their likeness, name, property or other rights without their permission, frequently for third party monetary gain. Similarly, individuals and legal entities operating online should be asked for permission for certain uses of their identity and personal data.

Like the first Principle, the duties in the second Principle are directed towards data flows for both incoming and outgoing transfers of data and communications across the identity “boundary.” These two directions of transfer relate to two separate traditional common law privacy torts. The second Principle’s duty to obtain permission for “all sharing of identity and personal data,” is similar to the common law tort of “misappropriation.” The duty to obtain permission for sending of communications to a Member is intended to prevent the separate harm of “unreasonable intrusion upon another’s seclusion.”

The Permission Principle is related to the Promise Principle, but reflects a different set of duties. This Permission Principle recognizes that the identity integrity established in the Promise Principle is not an impermeable barrier, but needs to be recognized as a “semi-permeable membrane”, i.e., one that permits data and communications to flow to and from Members. The second Principle simply requires that Members be involved in the decisions about how data flows to and from them, and that permission about those flows be obtained openly and honestly.

The Third Principle: Protection

Protection. *As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of identity and personal data shared with that Member.*

The third Principle represents each Member’s agreement to be bound by the duty to protect identity and personal data shared with that Member, specifically against unauthorized intrusions of a third party.

People in the physical world who depend on others to protect them from third party harm also need protection from harm caused by the failure of those others to perform those duties. In the physical world, this “duty to protect” varies greatly from one context to another, since the harms to be protected against also vary. There are many types of traditional legal actions that can result from a breach of duty to protect another person in various contexts. The more general, multi-context, legal concepts of “detrimental reliance” and “negligence” were developed to deal with the broader issues of compensating parties that are harmed because another party breached a duty to protect. In the latter case, the establishment of a duty (including a duty to protect someone’s person or property) could lead to liability for the person bound by the duty if such person breached the duty in a way that caused damages (such as when a hired security guard falls asleep on the job, allowing a robbery to take place).

The third Principle relates to the traditional common law privacy torts of unreasonable publicity disclosing details of another’s private life, and to negligence.

The Fourth Principle: Portability

***Portability:** As part of this promise, every Member agrees to ensure the portability of the identity and personal data shared with that Member.*

The fourth Principle represents each Member’s agreement to be bound by the duty to cause any identity and personal data shared with that Member to be portable, i.e., to be available to the data subject Member to easily copy or move to other contexts of the Member’s choosing.

Just as people in the physical world need to be able to move about freely, and to be protected from limitation of movement characterized in extreme cases as “kidnapping,” and “false imprisonment,” individuals and legal entities need to be able to access their digital identity and data about them online from a variety of services and in a variety of contexts. This Principle is directed at causing Members, in their role as data collectors and handlers, to respect other Members’ online identity integrity by granting such access.

The traditional harms of “false imprisonment” and “kidnapping” and in the consumer rights context “lack of consumer choice” are the roots of this principle.

The Fifth Principle: Proof

***Proof:** As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.*

The first four principles relate primarily to duties involving actions taken with respect to identity and personal data, whereas the Proof Principle focuses on maintaining information flows needed for operation of a reputation system that provides incentive for all Members to abide by, and encourage other Members to abide by, these Principles.

People in the physical world need protection from the harm to reputation called “defamation” and its twin torts “libel” (written defamation) and “slander” (spoken defamation). There is also the related common law privacy tort called “False Light,” where reputation is harmed by the juxtaposition of identity information about a person with other unrelated information that causes the impression of a relationship that can harm the person’s reputation.

The fifth principle creates a duty for all Members of the trust network to cooperate as peers in maintaining their reputations in order to prevent these same harms online.

The Respect Trust Framework Reputation System consists of two complementary parts: the Respect Vouching System for awarding positive reputation, and the Respect Conflict Resolution System for assigning negative reputation. The Respect Vouching System is defined in Exhibit A, and the Respect Conflict Resolution System is defined in Exhibit B.

Versioning and Amendments

Given that the purpose of the Respect Trust Framework is to help ensure trust among Members of a network, it is of utmost importance that the Members be able to rely on the integrity and stability of the trust framework itself. For that reason, any amendments to the Respect Trust Framework must be approved by the Members of the network according to the following rules.

1. All Members shall receive formal notice from Connect.Me of the vote via an electronic message delivered through the network, and a link to an electronic ballot with relevant information about the proposed amendment.
2. All Trust Anchor Members (as defined in Exhibit A) as of the time notice is issued shall be eligible to vote on the amendment. No other Members may vote.
3. The notice described in rule (1) above shall be made at least thirty (30) days prior to the voting deadline to permit Trust Anchor Members time to read, study, and debate the amendment.
4. Each Trust Anchor Member shall be allocated 100 votes.
5. A Trust Anchor Member may vote all of their own votes, or may assign any portion of their 100 votes to one or more other Trust Anchors to vote as their proxy, or any combination of these options.
6. There is no required quorum.
7. An amendment shall pass if it receives equal to or greater than a two-thirds supermajority of the votes cast. Otherwise it shall fail.
8. If the amendment passes, Connect.Me shall post and announce the amended version of the Respect Trust Framework to all Members within five business days. The terms of the new version shall be effective 30 days after the announcement.

Plug-In Trust Frameworks

The Respect Trust Framework is intended to provide an overarching set of principles and rules for protection of identity and personal data on a digital trust network. Groups of Members may desire to develop and apply more specific sets of principles and rules to more specific domains while still maintaining compatibility with the Respect Trust Framework. Such sets of principles and rules are called **Plug-In Trust Frameworks**. For a trust framework that normatively cross-references the Respect Trust Framework to qualify as a Plug-in Trust Framework, it must meet the following rules:

1. It must provide an explicit reference to the Respect Trust Framework.
2. It must not define principles or rules in conflict with the principles or rules defined in the Respect Trust Framework.
3. It must not redefine or require an alternate interpretation of the principles or rules defined in the Respect Trust Framework.

Copyrights and Trademarks

The Respect Trust Framework is copyright 2011 Respect Network Corporation dba Connect.Me.

The Respect Trust Framework™, The Respect Promise™, and Connect.Me™ are trademarks of Respect Network Corporation dba Connect.Me.

Respect Network Corporation
2182 12th Avenue, San Francisco, CA, 94116, USA

Exhibit A: The Respect Vouching System

The rules in this section define the Respect Framework Vouching System.

Definitions

1. **Member** means any legal person (e.g., individual, commercial, governmental, etc.) that has joined the trust network and agreed to the Respect Promise.
2. **Context** means a uniquely addressable digital representation of a semantic concept with which one or more Members of the network associate their digital identity. All contexts will be represented with at least a text label in all languages supported within the network. A context may also be represented by a visual icon or graphic.
3. **Community** means the set of Members associated with a specific Context.
4. **Vouch** means a signal of positive reputation in a specific Context given by one Member of the trust network about another Member. In the special context of Trust Anchor (defined below), a Vouch signals an expectation of conformity to the Respect Trust Framework. The meaning a Vouch in any other Context may be further defined by the Community governing that Context.
5. **Active Vouch** means a Vouch that is currently in force (i.e., has not been deleted).
6. **Voucher** means the Member making the Vouch.
7. **Recipient** means the Member that is the subject of the Vouch.
8. **Reputation Graph** is the publicly accessible view of the Contexts, Vouches given, and Vouches received for any Member.
9. **Trust Anchor** is the specific Context defined by the Respect Trust Framework in which Members may Vouch for other Members to signal an expectation of compliance with the Respect Trust Framework.
10. **Trust Anchor Status** is a trust level indicator in the Reputation Graph available only to Members who meet the qualifications defined below.

General Rules For Vouching

1. Any Member of the network may Vouch for any other Member in a Context to which they both agree. Without agreement of the Voucher and Recipient with regard to a Context, no Vouch shall be accepted.
2. All Vouches in a Context that is already part of a Member's public Reputation Graph will be public for both the Voucher and the Recipient.
3. A Vouch for a Recipient in a new Context, defined as a Context that is not yet part of the recipient's Reputation Graph, will not be public unless and until the Recipient approves the addition of that Context to their Reputation Graph.
4. Either a Voucher or a Recipient may unilaterally delete a Vouch at any time. If either party deletes the Vouch, it is removed from the Reputation Graph of both the Voucher and the Recipient.

Specific Rules for Trust Anchor Vouching

1. A Vouch in the Trust Anchor context is defined to have this specific meaning: "The Voucher believes the Recipient will keep The Respect Promise."
2. Only a Trust Anchor may be a Trust Anchor Voucher and make a Trust Anchor Vouch.
3. A Trust Anchor Voucher is limited to making a maximum of 150 Active Trust Anchor Vouches at any one time.
4. A Member who has received five Trust Anchor Vouches is eligible for Trust Anchor Status.
5. If the Member accepts Trust Anchors Status, the Member's Reputation Graph will indicate that the Member is a Trust Anchor and the Member is eligible to make Trust Anchor Vouches.
6. For any period that the number of Trust Anchor vouches for a Member drops below five, the Member shall lose Trust Anchors status. Trust Anchor status will be restored as soon as the number of Trust Anchor Vouches for that Member is five or more.
7. Vouches made by a Trust Anchor remain in effect even if the Voucher temporarily or permanently loses Trust Anchor status after making such Vouches.

Special Rules for Founding Trust Anchors

1. To populate the initial Membership of the Trust Anchor community, Connect.Me may appoint Founding Trust Anchors through the process described in rule (2) below. Such Appointments are to be made during the initial phase of Respect Network Member Community development on the same basis as Vouches and are subject to the same Conflict Resolution rules except as provided in this section.
2. A Founding Trust Anchor may be appointed in one of three groups:
 - a. As an individual invited to become a Founding Trust Anchor as a result of being known directly by a representative of Connect.Me or invited by such a representative at a conference focused on the Internet identity, privacy, and security industry.
 - b. As an individual known directly by the individuals in the first group, provided each individual in the first group is limited to a maximum of 20 appointments.
 - c. As an individual nominated through a public online nomination process conducted by Connect.Me on Twitter and subsequently verified by individuals in the first or second group.
3. Prior to becoming a founding Trust Anchor, the individual must: a) become a Member, and b) agree to accept appointment as a Founding Trust Anchor.
4. Founding Trust Anchors are not different than other Trust Anchors; this class of Trust Anchors exists only as a method of bootstrapping the trust network. Once the number of Members of the Trust Anchor community (including founding Trust Anchors) reaches or exceeds one million, founding Trust Anchor Anchors must meet the same Trust Anchor Vouch qualifications as all other Trust Anchors as defined above.

Exhibit B: The Respect Conflict Resolution System

The following rules apply to any Member of the Connect.Me Network filing a Complaint through the Respect Conflict Resolution Process Initiation Form and Complaint Form (the “Asserting Member”) and to any Member that receives such a Complaint while registered with the Connect.Me Network (the “Responding Member”) (collectively, the “Parties”).

1. Overview of the Respect Conflict Resolution Process

1.1. Agreement to Engage in Structured Negotiations and to Submit to Trust Anchor Panels

Connect.Me Network Members attempt in good faith to use the Respect Conflict Resolution Process to amicably resolve disputes among Members relating to the Respect Principles.

The Conflict Resolution Process takes place in two phases. Phase 1 consists of Structured Negotiations between the parties via the Connect.Me Dashboard. Phase 1 is completely voluntary and any resolution of a Complaint during Phase 1 must be by agreement of the parties.

Phase 2 is an Arbitration-style proceeding in which a panel of three Trust Anchors (“TA Panel”) evaluate the parties’ positions and evidence and make a binding decision as to how the Member’s Reputation Graph should be affected as a result of the conflict.

1.1. Claim Eligibility

The Respect Conflict Resolution Process is designed to address identity and personal data policies and practices that are viewed as not in conformance with the Respect Trust Framework. Claims for violation of law or for relief other than that explicitly stated above, including monetary and injunctive relief are outside the scope of the Respect Conflict Resolution Process and will not be considered.

1.2. Available Remedies

During Phase 1, the scope of available remedies is within the sole discretion of the Asserting and Responding Members who are charged with negotiating a solution to the dispute. During Phase 2, the only remedy available is an adjustment in the Members’ Reputation Graph. A TA Panel cannot direct corrective action that would require:

Relief in a form other than an adjustment to the Member’s Reputation Graph.

Relief in a form that would require the Responding Member to violate any legal requirements imposed on it by contract, statute, regulation or other legal authority.

1.3. Administration of Conflict Resolution Process: Dashboard

All communications defined in this document between the parties and, if the Complaint proceeds to Phase 2, the TA Panel, must take place via the Connect.Me Dashboard (“Dashboard”). Communications via other channels is not prohibited but is not formally part of the Respect Conflict Resolution Process as defined in this document.

All documentary evidence will be uploaded to the Dashboard of each Member and TA Panel Members involved. Members and TA Panelists may freely view the evidence via the Dashboard but are prohibited from copying it and/or storing its contents outside of the Connect.Me Network.

1.4. Responsibilities of Parties and TA Panels

The Asserting Member and Responding Member are responsible for continuing to seek to conform behaviors to the principles and rules defined in the Respect Trust Framework. This requires that Members cooperate with each other, Connect.Me, and the TA Panel in the pursuit of the resolution of the Complaint through each step of the Respect Conflict Resolution Process. The intention of the Process is to resolve conflict. It is for this reason that the scope of potential relief available through the process is kept narrow and specific, i.e., adjustments to the Respect Reputation System that are intended to indicate the level of such conformity to such rules.

The TA Panel is responsible for substantive review and ultimate decision on the merits of the Complaint. This role is performed by other Connect.Me Members that are qualified as Trust Anchors as defined in Exhibit A. TA Panel Members volunteer to help support the Network by participating in one or more TA Panels. To encourage and reward such service, Connect.Me is authorized to set a policy of awarding a form of positive reputation to the Reputation Graph of a Trust Anchor that successfully serves on a TA Panel. TA Panelists serve in the role of arbitrators, hearing the facts and reaching decisions that the Members agree will be binding; but solely with respect to the decision on whether or not to adjust the Responding Member's Reputation Graph, as that is the only remedy available in Phase 2.

1.5. Parties' Treatment of Information Received During the Process

By participating in the Conflict Resolution Process, the Asserting Member and the Responding Member agree that they will treat any information provided to them as having been provided exclusively for purposes of the Conflict Resolution Process and that they will not provide the material to anyone other than persons directly involved in the Conflict Resolution Process. Failure to do so may give rise to an additional Complaint.

1.6. Role of Connect.Me in Conflict Resolution Process

Connect.Me does not take a position in Member disputes and does not decide the outcome of these proceedings. When disputes proceed to Phase 2, those outcomes are determined by individual TA Panels and represent the view of the Connect.Me Network Member Community, not the company.

Connect.Me is not involved in reviewing, evaluating, investigating, analyzing and making a decision on the merits of an eligible Complaint. Notwithstanding the limitation on Connect.Me's authority to hear and decide Complaints, the Members agree that Connect.Me shall have access to all records associated with the Respect Conflict Resolution Process to help Connect.Me research and develop its processes to better serve Member interests.

2. Initiating the Respect Conflict Resolution Process

2.1. Filing a Complaint

The Conflict Resolution Process is initiated when an Asserting Member submits a valid and complete Complaint Form to Connect.Me Network via the Dashboard.

The Complaint should contain factual statements, clearly explain why the Asserting Member believes that the Responding Member does not conform to the Respect Trust Framework, and should not contain emotional or abusive declarations or statements that are defamatory or profane.

The Asserting Member has the option of including any documentary evidence that it believes supports its Complaint.

The Complaint Form must be validly completed by the Asserting Member and the information submitted by the Asserting Member must be sufficiently complete to permit the Responding Member and, if necessary, the TA Panel (in Phase 2) to be able to adequately evaluate the Complaint. Complaint Form submission is subject to automatic “machine” validation only. Connect.Me is not involved in the review of Complaint Forms.

2.2. Acceptance of Complaint into Respect Conflict Resolution Process

When the automated processes determine that the Complaint is valid, a copy of the Complaint will be provided to the Asserting Member with an acknowledgment of the Complaint via the Dashboard. A Notice of Complaint will be sent to the Responding Member simultaneously.

3. Phase 1

3.1 The Phase 1 Conflict Resolution Period

During Phase 1, the parties agree to attempt to resolve the conflict in good faith for a period of thirty (30) days from transmittal of the Notice of Complaint to the Responding Member (the “Phase 1 Period”). The Phase 1 Conflict Resolution Period may be extended only if both members submit a request for extension of time through the Dashboard. Phase 1 may be terminated prior to the completion of the Phase 1 Period at the request of either party.

3.2 The Responding Member’s Response

Within the Phase 1 Period, the Responding Member should acknowledge to the Asserting Member that it has received the Complaint. It is recommended that the Responding Member make a good faith effort to discuss the issues within the Scope of Conflict Resolution with the Asserting Member. In supporting its position, the Responding Party has the option of uploading documentary evidence that it believes supports its position.

Failure to respond within the allotted time will result in the Complaint automatically being escalated to Phase II. Failure to respond will also be noted in the Responding Member’s Reputation Graph.

3.3 Subsequent Phase 1 Proceedings

After the Responding Member submits its response the parties have the remainder of the Phase 1 Period to communicate with each other through the Dashboard and attempt to resolve the Complaint. They may exchange as many communications, and upload as much evidence, as they wish. However, in the event that the Asserting Member does not reply to a communication from the Responding Member within five (5) days, either by communication with the Responding Member via the Dashboard or by terminating the Complaint, the Complaint will be deemed abandoned.

3.4. Ending Phase 1

Phase 1 of Conflict Resolution is voluntary. Either Member can terminate the Phase 1 proceeding at any time during the Conflict Resolution Period.

3.4.1. Abandonment of Complaint

In the event that an Asserting Member fails to reply to the Responding Member’s response, the Complaint will be deemed abandoned and a notation will be made on the Asserting Member’s

Reputation Graph. All records of the Complaint will be deleted from the Responding Member's Reputation Graph.

3.4.2. Dismissal by the Asserting Member

The Asserting Member may voluntarily dismiss or terminate its Complaint during the Phase 1 Period by completing the Complaint Dismissal Form on the Dashboard. For example, it might do this if the matter is resolved by Agreement of the Asserting and Responding Members. The dismissal or termination of the Complaint by the Asserting Member during Phase 1 concludes the matter, and negates the need to move to Phase 2 of the Conflict Resolution Process. A notation will be made on each Member's Reputation Graph that the Complaint was settled in Phase 1.

3.4.3. Escalation by the Responding Member

The Responding Member cannot dismiss the Complaint. The Responding Member may, however, in its discretion, terminate the Phase 1 Conflict Resolution Period at any time during the Phase 1 Conflict Resolution Period. The termination of the Phase 1 Conflict Resolution Period by the Responding Member, or upon the expiration of the Conflict Resolution Period, does not terminate the Complaint, which is then moved to Phase 2 of the Conflict Resolution Process.

3.4.4. Escalation by the Asserting Member

The Asserting Member also has the option of escalating the dispute to Phase 2. Escalation may be appropriate if, for example, the Responding Member has been negotiating in bad faith and the Asserting Member does not believe that a resolution can be reached.

3.5. Administration of the Complaint following a Phase 1 Resolution

If the parties are able to resolve the Complaint during Phase 1, the Asserting Member will promptly submit the Phase 1 Resolution Form through the Dashboard.

3.6. Records of Phase 1 Proceedings

3.6.1. Communications Between the Parties

If a Complaint is terminated (whether through resolution or abandonment) during Phase 1, Connect.Me will delete all communications and documents related to the Complaint from the Dashboard when the Phase 1 Resolution Form is submitted. To improve the Respect Conflict Resolution Process, Connect.Me retains the right to retain a copy of these records on Connect.Me's servers for a period of three (3) years.

If a Complaint is escalated to Phase 2, all communications and postings will remain accessible through the Dashboard until Phase 2 is terminated. These communications and postings will be made available to the TA Panel once it has been chosen.

3.7. Reputation Graph Information

When a Complaint is filed, the Reputation Graph for the Responding Member will show that a Complaint is pending against the Responding Member. The details of the Complaint and the identity of the Asserting Member are not shown.

If the Complaint is resolved or abandoned during the Phase 1 Period, the record of a pending Complaint is deleted from the Responding Member's Reputation Graph. This restores the Responding Member's Reputation Graph to the same state as though the Complaint had never been filed.

If the Complaint is escalated to Phase 2 as a result of the Responding Member's failure to respond within the time provided by these rules, the Responding Member's Reputation Graph will record the refusal to mediate. No details of the Complaint shall be shown.

4. Phase 2

4.1. Initiation of Phase 2

A Complaint will automatically be considered to be listed for consideration and decision by a TA Panel in a Phase 2 if it is not resolved during Phase 1 or the parties choose to escalate it to Phase 2. At the time of listing, Connect.Me will automatically generate a Notice of Phase 2 ("Phase 2 Notice") that will be provided to the Asserting Member and Responding Member through the Dashboard.

4.2. Selection of the TA Panel

Within 48 hours of the initiation of Phase 2, a TA Panel of three Trust Anchors shall be assigned automatically to this dispute. In order to assure neutrality, TA Panel members may not have vouched for either party or vouched for another Member who has vouched for either party (i.e., they must be at least "two degrees removed"). In addition TA Panel members may not be employed by either party or otherwise have a conflict of interest in mediating the conflict.

Parties will be immediately informed of the assignment, provided links to the Profile Pages of each Member assigned to the TA Panel, and given 48 hours to object to any assignments and request replacements. In the event that an objection is made, a replacement will be automatic—there is no need to prove a conflict. To prevent parties from putting off resolution as they seek a more favorable TA Panel, each party is limited to three (3) objections and as soon as 48 hours has passed without a single objection, the TA Panel is set and a Notice of Final Panel Selection will be sent to the Parties via the Dashboard.

4.3. TA Panel Procedures

Once a TA Panel has been set, all members of the TA Panel will receive access to the Asserting Member's Complaint through the Dashboard. All subsequent communications between the parties and the TA Panel will be via the Dashboard and the same rules regarding copying materials will apply as in Phase 1.

4.4. Responding Member's Response to a Complaint

The Responding Member shall have five (5) days from the date of the Notice of Final Panel Selection or twenty (20) days from the Phase 2 Notice, whichever comes first, to file a written response to the Complaint in the form of either an Answer or Motion to Dismiss.

4.4.1. Answer

The Answer shall describe facts and provide information to support the Responding Member's responses to the Complaint. The Responding Member also has the option uploading documentary evidence (not already submitted during Phase 1) in support of its position. The Responding Member shall submit the Answer via the Dashboard where it will be made available to the Answering Party and the TA Panel members.

4.4.2. Motion to Dismiss

If a Responding Member believes that a Complaint is improper because the Complaint either (i) raises issues solely outside of the Respect Principles or (ii) is frivolous, duplicative or harassing, the Responding Member shall file a motion to dismiss that briefly explains why the Complaint is improper and should not be considered.

A TA Panel has full discretion to decide whether to grant or deny a Motion to Dismiss. For purposes of deciding such a motion, a complaint is frivolous if the TA Panel determines that the facts alleged either could not be true or, even if true, would not constitute a violation of the Respect Trust Framework. A Complaint is duplicative and harassing if the same member has filed a complaint alleging the exact same conduct by the same Responding Member. A Complaint is not duplicative, however, if the complaint alleges that the Responding Member continues to engage in conduct that a previous TA Panel has already determined is contrary to the Respect Trust Framework.

If a Motion to Dismiss is granted, the record of the Complaint will be deleted from the Responding Member's Reputation Graph and a notation will be made on the Asserting Member's Reputation Graph.

4.5. Responding Member Failure to Respond to a Complaint

If a Responding Member fails to file a substantive written Answer to the Complaint within the period provided in these Rules, or otherwise fails to provide a timely response to a Connect.Me or TA Panel request for further information, the Responding Member shall be considered to have "defaulted" in the matter. In the case of a Responding Member default, Connect.Me will advise the Responding Member that the default will be recorded in the Responding Member's Reputation Graph.

The Panel will then consider the facts alleged in the Complaint and any documentary evidence submitted during Phase 1 in issuing its decision on the merits. The Panel has the discretion to adjust Responding Party's Reputation Graph to reflect the failure to respond.

4.6. Asserting Member's Reply to Responding Member's Answer

The Asserting Member has ten (10) days after receipt of the Answer to provide a written reply (the "Reply") to the Answer. If the Asserting Member does not provide either a Reply or a notification that it wishes to proceed with the case but elects not to file a Reply, the TA Panel shall close the matter following the expiration of the Asserting Member's time to reply. All references to the Complaint shall then be deleted from the Responding Member's Reputation Graph and the Asserting Member's Reputation Graph shall be updated to reflect the abandoned Complaint.

4.7. Request For Additional Information

If a TA Panel, in its sole judgment, concludes that additional information is needed to enable a full and fair review, evaluation, investigation, analysis, and decision on the merits of an eligible Complaint review, it shall promptly contact the Asserting Member or the Responding Member, as the case may be, with such request.

For information requests made of the Asserting Member, if the TA Panel receives the requested information within ten (10) days of its request, it will proceed with the hearing. If the TA Panel does not receive the requested information within ten (10) days of its request, it will notify the Asserting Member that it cannot proceed with the Complaint and the Complaint shall be dismissed. The Responding Member's Reputation Graph shall be updated to remove all references to the Complaint. The Asserting Member's Reputation Graph will be updated to reflect that the complaint has been abandoned.

If the request for additional information is made by the TA Panel to the Responding Member, the Responding Member is required to respond with the requested information within ten (10) days of the request. If the Responding Member does not timely respond, a notation will be made on the Responding Member's Reputation Graph and the Panel will make a decision based on the information available to it.

To keep the process focused on the issues as determined by the TA Panel, no response to this information is permitted unless requested by the Panel.

If a Member fails to respond to the TA Panel request for additional information or comments or fails to respond to the other Member's submission in response to such request, the TA Panel shall proceed with its consideration of the Complaint, and it may take into account the lack of response to its request as a factor, giving it such weight as the TA Panel deems appropriate.

4.8. TA Panel Decisions

Where a TA Panel has heard a Complaint and has not closed the matter because of the Responding Member's nonparticipation, it shall finalize its decision and submit it to the parties via the Dashboard.

The TA Panel will finalize its decision by the later of fourteen (14) days of its receipt of the final document received from the Members, or the expiration of the time limit for receiving such document. The decision shall briefly summarize the facts, whether the Panel concluded that there had been a violation of the Respect Principles, and the Panel's reasoning for the particular judgment imposed. The votes of individual Panel members shall not be made public but if one panel member disagrees with the appropriate outcome, he or she may submit a brief dissent explaining his or her position. It shall then promptly provide a copy of such decision to all parties.

Where a finding is made against Responding Member and the TA Panel concludes that a negative adjustment will be made in the Reputation Graph of the Responding Member, the TA Panel shall make that adjustment via their Dashboard.

Where the TA Panel concludes that no negative adjustment will be made to the reputation score of the Responding Member as a result of the allegations made in the Complaint, but that the Complaint had valid grounds for being considered, the TA Panel will dismiss the Complaint and all record of the Complaint shall be deleted from the Reputation Graph of both the Asserting and Responding Members.

Where the TA Panel concludes that no negative adjustment will be made to the reputation score of the Responding Member as a result of the allegations made in the Complaint, and that the Complaint did not have grounds for being considered because it was false, malicious, frivolous, or otherwise intended only to undeservedly harm the reputation of the Responding Member, the TA Panel will dismiss the Complaint and all record of the Complaint shall be deleted from the Reputation Graph of the Responding Member, and the TA Panel shall make a negative adjustment the reputation graph of the Asserting Member.

The Members agree that by joining Connect.Me Network they are subjecting themselves to the Respect Reputation System, which is designed, developed, and deployed to have the authority of the system reside in the Connect.Me Network Member Community. Connect.Me provides the platform from which Members can act to independently exercise their judgment about the application of the Respect Principles based on their individual and contextual framework, but with attention also to the goals of more uniform application of the Respect Principles where possible and appropriate.

4.9. No Appeal of TA Panel Decisions

The decisions of the TA Panel are final and no appeal is available under the Respect Conflict Resolution Process.

The absence of an appeal right under the Respect Conflict Resolution Process does not preclude or prejudice the ability of a Member to seek separate relief pursuant to applicable law or regulation, or any additional forms of relief that may be available to Members.

4.10. No Confidentiality of TA Panel Files

A TA Panel decision regarding a Complaint is the only permanent record of a Complaint or the process through which it was reviewed and decided. Other filings and communications will be retained by Connect.Me for a period of three (3) years but will not be easily accessible and will not be provided to anyone except in the case of compelled requests, such as upon Court order. There will be no record of proceedings.

4.11. Hold Harmless for Trust Anchors on TA Panels

The parties and all Members shall, jointly and severally, indemnify and hold harmless, Connect.Me and the individual members of the TA Panel, from any and all fees, costs and expenses (including but not limited to attorneys fees) for any act or omission in connection with any Conflict Resolution Process conducted under these procedures.

5. General Terms Applicable to Phase 1 and Phase 2 of the Respect Conflict Resolution Process

5.1. Use of Confidential Information Prohibited.

A Responding Member or Asserting Member may only submit information to Connect.Me that is not confidential or proprietary. Members should assume that all information provided to Connect.Me or to a TA Panel as part of the Conflict Resolution Process may be available to third parties. All materials provided to a TA Panel or Connect.Me are deemed to be non-confidential, and TA Panel Members and Connect.Me are under no obligation to maintain the confidentiality of any materials that they receive.

5.2. Publication of Conflict Resolution Statistics

Connect.Me shall publish Connect.Me Complaint statistics at least once each year, summarizing matters concluded during the previous period. These reports shall provide a statistical summary of

the number and nature of Complaints filed and accepted

the number of cases resolved during Phase 1

the number of improper complaint (i.e., those dismissed on motion to dismiss)

the number of complaints resolved against the Asserting Party

the number of complaints resolved against the Responding Party

as well as any other statistical information that Connect.Me determines should be collected and published. All information will be collected and published in the aggregate and will not reflect decisions of individual Complaints.

5.3. Timely Filings

For any submission under these Rules to be considered timely, it must be received by the Member's Dashboard within the period set forth in these Rules. Members may agree between themselves to extend the time limits specified in this section. In such case, the limits agreed to by the Members will be communicated via their Dashboards. Connect.Me shall not be involved in these communications other than the delivery of the electronic messages. Any Member filing or request made after the specified time limits will be considered untimely and will not be considered by the TA Panel.

5.5. General Record Retention Policy

Connect.Me may retain all Complaints (including purged Complaints), filings, Reputation Graph records and other communications related to the Respect Conflict Resolution Process for a period of three (3) years following initiation of a Complaint. Connect.Me may disclose such records to comply with legal process (e.g., a warrant, subpoena or court order) or law enforcement investigations.

5.6. Status as Private Settlement Discussions.

To facilitate settlement discussions, both parties agree that all communications between them during both the Phase 1 and Phase 2 Conflict Resolution Periods within the Scope of Conflict Resolution are “For Settlement Purposes Only” under United States Federal Rule of Evidence 408 (and state law counterparts and similar laws of other jurisdictions) not admissible into evidence in any proceeding brought by one Member against the other. The parties will not disclose such communications except to their attorneys and confidential advisers, or to comply with a subpoena, warrant or court order.

5.7. Right to Rely on Instructions.

Connect.Me may act in reliance upon any instruction, information, document, filing, name, email address or Asserting Member password that meets Connect.Me Network’s automated criteria.

Connect.Me Network may assume a person entering a Member identifier and the associated authentication credential is the purported Asserting Member or is authorized to act on their behalf.

Members authorize Connect.Me to assume that the latest communications addresses on file with Connect.Me Network are accurate and current.

5.8. No Warranties

CONNECT.ME DOES NOT WARRANT THIS CONFLICT RESOLUTION SERVICE. ALL INFORMATION, COMMUNICATIONS, FEATURES AND SERVICES ARE PROVIDED AS-IS AND AS-AVAILABLE WITHOUT WARRANTY OF ANY KIND. ALL WARRANTIES, INCLUDING MERCHANTABILITY, QUALITY, INTEGRATION, ACCURACY, TITLE AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED.

5.9. Connect.Me Network is Not Your Lawyer

CONNECT.ME DOES NOT PROVIDE LEGAL ADVICE OR LEGAL PROFESSIONAL SKILL OR JUDGMENT, IS NOT A “LAWYER” OR “JUDGE” PROVIDING LEGAL ADVICE OR JUDICIAL SERVICES, AND DOES NOT REPLACE YOUR ATTORNEY. RESPECT CONFLICT RESOLUTION SERVICES DO NOT ESTABLISH AN ATTORNEY CLIENT, FIDUCIARY OR OTHER PROFESSIONAL RELATIONSHIP.

5.10. No Liability

IN ADDITION TO ANY OTHER LIMITATION OF LIABILITY UNDER THE CONNECT.ME TERMS, CONNECT.ME DISCLAIMS LIABILITY FOR ANY LOSS OR DAMAGE, INCLUDING DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES (INCLUDING LOST SAVINGS, LOST PROFIT OR ATTORNEY FEES) AND WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE.

5.11. Indemnity

THE ASSERTING MEMBER AND THE RESPONDING MEMBER WILL DEFEND, INDEMNIFY AND HOLD CONNECT.ME HARMLESS FROM ANY CLAIM, LOSS OR DAMAGE ARISING OUT OF OR

RELATING TO RESPECT CONFLICT RESOLUTION SERVICES OR OTHER SERVICES OR FEATURES.

5.12. Protected Parties

THE DISCLAIMERS, LIMITATIONS, INDEMNITIES AND PROTECTIONS CONTAINED IN THESE RULES PROTECT CONNECT.ME, ITS OFFICERS, OWNERS, AGENTS, CONSULTANTS, ADVISERS, EMPLOYEES, AFFILIATES, ADVERTISERS, DISTRIBUTORS, PUBLISHERS AND PROMOTERS.

5.13. Parties Waiver of Subpoena Rights and of Liability Claims

By participating in the Respect Conflict Resolution Process, the Members agree that they will not subpoena the staff of Connect.Me, its Board members, or advisors, or any records of Connect.Me in any subsequent legal proceeding arising out of the matters at issue in the process in which they are participating. They also agree that Connect.Me, its staff, Board members and advisors shall not be liable for any act or omission in connection with the online Conflict Resolution Process.

5.14. Limitation of Remedies

Members agree that if Connect.Me breaches the Respect Conflict Resolution Rules or otherwise violates Member's rights, the sole and exclusive remedy will be to terminate the relationship with Connect.Me and the Respect Conflict Resolution Process. This applies regardless of whether the remedy fails of its essential purpose.

5.15. Miscellaneous

The Connect.Me Terms apply to these Rules.

Exhibit C: Comparison of the Respect Principles and FIPPs

This Exhibit provides a comparison of the five Respect Principles in the Respect Trust Framework with Fair Information Practices Principles from around the world.

Duty on Member	Right	Canada	Sweden	COP (Great Britain)	EU	EU	NSTIC	COE
					EU - 95/46/EC	EU-2002/58/EC		
Respect other Members' input and output controls	Identity Integrity	C-3 C-4 C-6 C-9	SW-1 SW-5 SW-6 SW-7 SW-8 SW-9	COP-1 COP-3 COP-4 COP-5 COP-8 COP-9 COP-10	EU 95-1 EU 95-3 EU 95-4 EU 95-5	EU 02-1 EU 02-2 EU 02-3 EU 02-4 EU 02-5 EU 02-6 EU 02-7	N-1 N-4	COE-1 COE-2 COE-3 COE-4 COE-5 COE-6 COE-9 COE-10
Ask permission before using or sending data/identity, Honest Dealing	Negotiation	C-2 C-3 C-5	SW-3 SW-4	COP-1 COP-2	EU 95-2	EU 02-2 EU 02-3 EU 02-4 EU 02-5 EU 02-6 EU 02-7	N-2 N-3 N-5 N-6	COE-2 COE-8 COE-11
Protect data/identity in possession from third parties	Safety from third party access	C-7	SW-9	COP-6 COP-7 COP-8	EU 95-5	EU 02-1 EU 02-3	N-4 N-7	COE-5 COE-6 COE-7
Allow data subject access and use of data/identity held about them	Freedom of movement	C-9						COE-9
Information sharing, cooperation	Fair systems information access, knowledge	C-1 C-8 C-9 C-10	SW-7	COP-9		EU 02-6	N-1 N-6 N-8	

Duty on Member	Right	OECD	HEW-1	PPSC	FTC	OITF	DHS	APEC	GSMA
Respect other Members' input and output controls	Identity Integrity	OECD-1 OECD-2 OECD-3 OECD-6	HEW-1 HEW-2 HEW-4 HEW-5	PPSC-1 PPSC-2 PPSC-3 PPSC-4 PPSC-5 PPSC-6 PPSC-7	FTC-3 FTC-4	OITF-1 OITF-3 OITF-4 OITF-7	DHS-2 DHS-3 DHS-4 DHS-6 DHS-7	A-1 A-2 A-3 A-4 A-6 A-8	GSMA-1 GSMA-2 GSMA-4 GSMA-8
Ask permission before using or sending data/identity, Honest Dealing	Negotiation	OECD-1 OECD-3 OECD-4 OECD-7	HEW-3	PPSC-4 PPSC-6 PPSC-8	FTC-1 FTC-2	OITF-7	DHS-2 DHS-6 DHS-8	A-2 A-3 A-4 A-5 A-9	GSMA-1 GSMA-2 GSMA-3 GSMA-5 GSMA-7
Protect data/identity in possession from third parties	Safety from third party access	OECD-5	HEW-5	PPSC-7 PPSC-8	FTC-4	OITF-9	DHS-5	A-1 A-7 A-9	GSMA-4 GSMA-6 GSMA-8
Allow data subject access and use of data/identity held about them	Freedom of movement	OECD-7		PPSC-2		OITF-6		A-8	GSMA-5
Information sharing, cooperation	Fair systems information access, knowledge	OECD-6 OECD-7 OECD-8		PPSC-1 PPSC-2 PPSC-8	FTC-3	OITF-2 OITF-4 OITF-8 OITF-10 OITF-11 OITF-12	DHS-1	A-2 A-9	GSMA-1 GSMA-9

RESPECT TRUST FRAMEWORK	
R-1	PROMISE: Every Member promises to respect the right of every other Member to control the identity and personal data they share within the network and the communications they receive within the network.
R-2	PERMISSION: As part of this promise, every Member agrees that all sharing of identity and personal data and sending of communications will be by permission, and to be honest and direct about the purpose(s) for which permission is sought.
R-3	PROTECTION: As part of this promise, every Member agrees to provide reasonable protection for the privacy and security of identity and personal data shared with that Member.
R-4	PORTABILITY: As part of this promise, every Member agrees to ensure the portability of the identity and personal data shared with that Member.
R-5	PROOF: As part of this promise, every Member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.

CANADA	
C-1	ACCOUNTABILITY: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
C-2	IDENTIFYING PURPOSES: The purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.
C-3	CONSENT: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
C-4	LIMITING COLLECTION: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
C-5	LIMITING USE, DISCLOSURE, AND RETENTION: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
C-6	ACCURACY: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
C-7	SAFEGUARDS: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
C-8	OPENNESS: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
C-9	INDIVIDUAL ACCESS: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended.
C-10	CHALLENGING: Compliance an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

SWEDEN	
SW-1	The controller shall, inter alias, ensure that personal data is only processed if it is lawful.
SW-2	The controller shall, inter alia, ensure that personal data is processed in a proper manner and in accordance
SW-3	The controller shall, inter alia, ensure that personal data is gathered only for specific, explicitly stated and legitimate purposes.
SW-4	The controller shall, inter alia, ensure that personal data is not processed for any purpose that is incompatible with that for which the data was gathered.
SW-5	The controller shall, inter alia, ensure that personal data that is treated is adequate and relevant to the purpose of the processing.
SW-6	The controller shall, inter alia, ensure that personal data is only processed if it is necessary having regard to the purpose of the processing.
SW-7	The controller shall, inter alia, ensure that personal data which is processed is correct and, if it is necessary, up-to-date.
SW-8	The controller shall, inter alia, ensure that personal data is rectified, blocked or erased, if it is incorrect or incomplete having regard to the purpose of the processing.
SW-9	The controller shall, inter alia, ensure that personal data is not kept for a longer period than is necessary.

GREAT BRITAIN (COP)	
COP -1	Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes.
COP-2	Access to information should be confined to those authorized to have it for the purpose for which it was supplied.
COP-3	The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose.
COP-4	In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs for separating identities from the rest of the data.
COP-5	There should be arrangement whereby the subject could be told about the information held concerning him.
COP-6	The level of security to be achieved by a system should be specified in advance by the user and should include precautions against deliberate abuse or misuse of information.
COP-7	A monitoring system should be provided to facilitate the detection of any violation of the security system.
COP-8	In the design of information systems, periods should be specified beyond which the information should not be retained.
COP-9	Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.
COP-10	Care should be taken in coding value judgments.

EU DATA DIRECTIVE (95/46/EC)	
EU 95-1	Member States shall provide that personal data must be processed fairly and lawfully.
EU 95-2	Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.
EU 95-3	Member States shall provide that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
EU 95-4	Member States shall provide that personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
EU 95-5	Member States shall provide that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

EU DATA DIRECTIVE (2002/58/EC)

EU 02-1	<p>Article 4 - Security</p> <p>1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented. (Article 4, Security)</p> <p>2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved. (Article 4, Security)</p>
EU 02-2	<p>Article 5 -Confidentiality of the communications</p> <p>1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality. (Article 5, Confidentiality)</p> <p>2. Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. (Article 5, Confidentiality)</p> <p>3. Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. (Article 5, Confidentiality)</p>

<p>EU 02-3</p>	<p>Article 6 - Traffic data</p> <p>1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1). (Article 6, Traffic data)</p> <p>2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued. (Article 6, Traffic data)</p> <p>3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time. (Article 6, Traffic data)</p> <p>4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3. (Article 6, Traffic data)</p> <p>5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities. (Article 6, Traffic data)</p> <p>6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes. (Article 6, Traffic data)</p>
<p>EU 02-4</p>	<p>Article 8 - Presentation and restriction of calling and connected line identification</p> <p>1. Where presentation of calling line identification is offered, the service provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the</p>

	<p>calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis. (Article 8, Caller ID)</p> <p>2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls. (Article 8, Caller ID)</p> <p>3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber. (Article 8, Caller ID)</p> <p>4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user. (Article 8, Caller ID)</p> <p>5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries. (Article 8, Caller ID)</p> <p>6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4. (Article 8, Caller ID)</p>
<p>EU 02-5</p>	<p>Article 9 - Location data other than traffic data</p> <p>1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. (Article 9, Location data)</p> <p>2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or</p>

	<p>subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication. (Article 9, Location data)</p> <p>3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service. (Article 9, Location data)</p>
<p>EU 02-6</p>	<p>Article 12 - Directories of subscribers</p> <p>1. Member States shall ensure that subscribers are informed, free of charge and before they are included in the directory, about the purpose(s) of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory. (Article 12, Directories)</p> <p>2. Member States shall ensure that subscribers are given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory, and to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge. (Article 12, Directories)</p> <p>3. Member States may require that for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers. (Article 12, Directories)</p> <p>4. Paragraphs 1 and 2 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to their entry in public directories are sufficiently protected. (Article 12, Directories)</p>
<p>EU 02-7</p>	<p>Article 13 - Unsolicited communications</p> <p>1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. (Article 13, Unsolicited communications). (Article 13, Unsolicited</p>

communications)

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use. (Article 13, Unsolicited communications)

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation. (Article 13, Unsolicited communications)

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited. (Article 13, Unsolicited communications)

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected. (Article 13, Unsolicited communications)

NSTIC	
N-1	TRANSPARENCY: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information. (PII)
N-2	INDIVIDUAL PARTICIPATION: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.
N-3	PURPOSE SPECIFICATION: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
N-4	DATA MINIMIZATION: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
N-5	USE LIMITATION: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.
N-6	DATA QUALITY AND INTEGRITY: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
N-7	SECURITY: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
N-8	ACCOUNTABILITY AND AUDITING: Organizations should be accountable for complying with these principles, providing training to all employee and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

COUNCIL OF EUROPE (COE)	
COE -1	Personal data undergoing automatic processing shall be obtained and processed fairly and lawfully.
COE-2	Personal data undergoing automatic processing shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.
COE-3	Personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.
COE-4	Personal data undergoing automatic processing shall be accurate and, where necessary, kept up to date.
COE-5	Personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
COE-6	Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.
COE-7	Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.
COE-8	Any person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.
COE-9	Any person shall be enabled to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form.
COE-10	Any person shall be enabled to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention.
COE-11	Any person shall be enabled to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

OECD	
OECD-1	COLLECTION LIMITATION PRINCIPLE: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
OECD-2	DATA QUALITY PRINCIPLE: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
OECD-3	PURPOSE SPECIFICATION PRINCIPLE: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
OECD-4	USE LIMITATION PRINCIPLE: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.
OECD-5	SECURITY SAFEGUARDS PRINCIPLE: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
OECD-6	OPENNESS PRINCIPLE: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
OECD-7	INDIVIDUAL PARTICIPATION PRINCIPLE: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
OECD-8	ACCOUNTABILITY PRINCIPLE: A data controller should be accountable for complying with measures which give effect to the principles stated above.

HEW 1	
HEW 1	There must be no personal data record keeping systems whose very existence is secret.
HEW 2	There must be a way for an individual to find out what information about him is in a records and how it is used.
HEW 3	There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
HEW 4	There must be a way for an individual to correct or amend a record of identifiable information about him.
HEW 5	Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse.

PPSC	
PPSC-1	The Openness Principle – There shall be no personal data record keeping system whose very existence is secret and there shall be a policy of openness about an organization’s personal data record keeping policies, practices and systems.
PPSC-2	The Individual Access Principle – An individual about whom information is maintained by a record keeping organization in individually identifiable form shall have a right to see and copy that information.
PPSC-3	The Individual Participation Principle – An individual about whom information is maintained by a record keeping organization shall have a right to correct or amend the substance of that information.
PPSC-4	The Collection Limitation Principle – There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information.
PPSC-5	The Use Limitation Principle – There shall be limits on the internal uses of information about an individual within a record keeping organization.
PPSC-6	The Disclosure Limitation Principle – There shall be limits on the external disclosures of information about an individual a record keeping organization may make.
PPSC-7	The Information Management Principle – A record keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate.
PPSC-8	The Accountability Principle – A record keeping organization shall be accountable for its personal data record keeping policies, practices, and systems.

FTC	
FTC-1	Notice: data collectors must disclose their information practices before collecting personal information from consumers
FTC-2	Choice: consumers must be given option with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided
FTC-3	Access: consumers should be able to view and contest the accuracy and completeness of data collected about them
FTC-4	Security: data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use

OITF WP	
OITF-1	Lawfulness: OITF Providers are responsible for ensuring that the technical, operational, and legal requirements of the OITF are consistent with the laws of the jurisdiction(s) where parties use it to conduct exchanges involving identity information.
OITF-2	<p>Open reporting and publication: OITF Providers must produce periodic reports on the operation and governance of the trust framework.</p> <p>They must ensure that a web site devoted to the OITF provides easy and timely access to</p> <ul style="list-style-type: none"> (a) the periodic reports, (b) all agreements that constitute the legal structure of the trust framework, (c) all policies and procedures by which the OITF operates (including criteria and processes for certification), (d) a plain-language explanation of the trust framework’s trust characteristics (for example, data protection strengths and weaknesses), and (e) records of dispute resolution activities and their results. However, publication is not required for assessment reports. <p>OITF Providers must ensure that all parties to agreements under the OITF have visibility into who is participating in it and in what capacity.</p>
OITF-3	<p>Ombudsmen: OITF Providers must ask governments where they do business to designate independent ombudsmen whose role is to look after the interests of individual users under their respective jurisdictions, and they must ensure that the OITF is designed to allow these ombudsmen to do their job.</p> <p>If law requires the sharing of identity information (including biometric data, behavioral data, and social graphs) without the informed consent of the person in question, parties to the OITF who are ordered to share this information must involve the ombudsmen.</p>
OITF-4	<p>Anti-circumvention and open disclosure: OITF participant must not be party to any side agreements that compromise the integrity of commitments under the trust framework.</p> <p>If a participant is party to any agreements that might otherwise conflict with obligations under the trust framework, that party must disclose the existence and nature of these agreements to the affected party or parties at the earliest opportunity.</p> <p>OITF Providers and assessors must disclose all their agreements and the terms of those agreements.</p>
OITF-5	<p>Non-discrimination. Participants in the OITF must avoid discrimination.</p> <p>Participants must not engage in exclusive dealing arrangements relating to the trust framework.</p>
OITF-6	Interoperability. Software and hardware specified in the technical requirements of an OITF must conform to defined standards that promote interoperability.
OITF-7	Open Versioning: OITF Providers must spell out how new versions of the OITF

	will be decided, when they will be published, how participants will be transitioned to these new versions, and how the interests of participants in the OITF will be protected.
OITF-8	Participant Involvement: OITF Providers must enable participants to share contact details so that they may convene virtually to discuss matters related to the trust framework.
OITF-9	Data Protection. Participants in OITFs will adhere to data protection practices at least as strong as those of the OECD's Privacy Guidelines (Part Two in its entirety, concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).
OITF-10	Accountability: OITF Providers must state on a publicly accessible web site how the OITF provides accountability to all participants, including the users whose identity information will be exchanged under it.
OITF-11	Auditability: OITF Providers must ensure that all parties to agreements under the trust framework, including themselves, agree to be subject to audit for conformance with these Principles of Openness.
OITF-12	Redress. OITF Providers must ensure that all agreements under the OITF afford the parties an effective right and mechanism to seek redress. Redress. OITF Providers must ensure that all agreements under the OITF afford the parties an effective right and mechanism to seek redress.

DHS	
DHS-1	Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PH, and auditing the actual use of PH to demonstrate compliance with these principles and all applicable privacy protection requirements.
DHS-2	Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
DHS-3	Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
DHS-4	Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PH for as long as is necessary to fulfill the specified purpose(s).
DHS-5	Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
DHS-6	Use Limitation: DHS should use PH solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
DHS-7	Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
DHS-8	Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

APEC	
A-1	<p>PREVENTING HARM: Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information.</p> <p>Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.</p>
A-2	<p>NOTICE: Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:</p> <ul style="list-style-type: none"> a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organization to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information. <p>All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information.</p> <p>Otherwise, such notice should be provided as soon after as is practicable.</p> <p>It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information.</p>
A-3	<p>COLLECTION LIMITATION: The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.</p>
A-4	<p>USES OF PERSONAL INFORMATION: Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:</p> <ul style="list-style-type: none"> a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.
A-5	<p>CHOICE: Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.</p> <p>It may not be appropriate for personal information controllers to provide these</p>

	mechanisms when collecting publicly available information.
A-6	INTEGRITY OF PERSONAL INFORMATION: Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
A-7	<p>SECURITY SAFEGUARDS: Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses.</p> <p>Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.</p>
A-8	<p>ACCESS AND CORRECTION: Individuals should be able to:</p> <p>a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;</p> <p>b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;</p> <p style="padding-left: 40px;">i. within a reasonable time;</p> <p style="padding-left: 40px;">ii. at a charge, if any, that is not excessive;</p> <p style="padding-left: 40px;">iii. in a reasonable manner;</p> <p style="padding-left: 40px;">iv. in a form that is generally understandable; and</p> <p>c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.</p> <p>Such access and opportunity for correction should be provided except where:</p> <p style="padding-left: 40px;">(i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;</p> <p style="padding-left: 40px;">(ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or</p> <p style="padding-left: 40px;">(iii) the information privacy of persons other than the individuals would be violated.</p> <p>If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.</p>
A-9	<p>ACCOUNTABILITY: A personal information controller should be accountable for complying with measures that give effect to the Principles stated above.</p> <p>When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.</p>

GSMA	
GSMA-1	<p>OPENNESS, TRANSPARENCY AND NOTICE: Responsible persons shall be open and honest with users and will ensure users are provided with clear, prominent and timely information regarding their identity and data privacy practices.</p> <p>Users shall be provided with information about persons collection personal information about them, the purposes of an application or service, and about the access, collection, sharing and further use of a users' personal information, including to whom their personal information may be disclosed, enabling users to make informed decisions about whether to use a mobile application or service.</p>
GSMA-2	<p>PURPOSE AND USE: The access, collection, sharing, disclosure and further use of users' personal information shall be limited to meeting legitimate business purposes, such as providing applications or services as requested by users, or to otherwise meet legal obligations.</p>
GSMA-3	<p>USER CHOICE AND CONTROL: Users shall be given opportunities to exercise meaningful choice, and control over their personal information.</p>
GSMA-4	<p>DATA MINIMIZATION AND RETENTION: Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop applications and services should be collected and otherwise accessed and used.</p> <p>Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous.</p>
GSMA-5	<p>RESPECT USER RIGHTS: Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information.</p>
GSMA-6	<p>SECURITY: Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information.</p>
GSMA-7	<p>EDUCATION: Users should be provided with information about privacy and security issues and ways to manage and protect their privacy.</p>
GSMA-8	<p>CHILDREN AND ADOLESCENTS: An application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information is appropriate in all given circumstances and compatible with national law.</p>
GSMA-9	<p>ACCOUNTABILITY AND ENFORCEMENT: All responsible persons are accountable for ensuring these principles are met.</p>