

The Respect Trust Framework™

VERSION 1 BETA 2011-08-15

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 share identity and personal data with greater confidence that it will be protected 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 for both positive reputation (called vouching) and negative reputation (called complaints). The rules for this Respect Reputation System 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 purpose, principles, and rules 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: VERSION 1 BETA	3
PURPOSE	4
PRINCIPLES	4
THE PROMISE PRINCIPLE	5
THE PERMISSION PRINCIPLE	6
THE PROTECTION PRINCIPLE	6
THE PORTABILITY PRINCIPLE	7
THE PROOF PRINCIPLE	7
THE RESPECT REPUTATION SYSTEM™	8
DEFINITIONS	8
TRUST LEVELS	9
ACCOUNTABILITY RULES	10
VOUCHING RULES	10
COMPLAINT RULES	11
LOCAL TERMS	12
PLUG-IN TRUST FRAMEWORKS	12
VERSIONING AND AMENDMENTS	13
COPYRIGHTS AND TRADEMARKS	13
EXHIBIT C: COMPARISON OF THE RESPECT PRINCIPLES AND FIPPS	14

Status: Version 1 Beta

This version of the Respect Trust Framework was submitted by [Connect.Me](#) on 15 August 2011 for public listing with the Open Identity Exchange (OIX)¹ as a digital trust framework in accordance with the [Open Identity Trust Framework \(OITF\) 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 for an increase in the level of control that all legal persons (both individuals and organizations) have over their digital identity and personal data.

Connect.Me serves as the provider of the Respect Network™, which incorporates the Respect Trust Framework into its Member contract. The Respect Trust Framework may only be modified by trusted members of the Respect Network as provided for in the Versioning and Amendments section of this document. This ensures that future evolution of the Respect Trust Framework only happens with the input and consent of the Members, a requirement which fulfills the Open Versioning Principle, one of the twelve Principles of Openness as defined in the OITF Model.

As described in the Local Terms section of this document, each Member of the Respect Network has the authority to decide the local terms that apply to specific relationships with other Members provided they do not conflict with the global terms defined in this Respect Trust Framework. This applies to Connect.Me as well, i.e., Connect.Me as the network provider is subject to the Respect Trust Framework in the same way as every other Member. Thus, Connect.Me's Local Terms must be entirely consistent with the Respect Trust Framework. Connect.Me's Local Terms include its Terms of Service and Privacy Policy. Members exercise their authority regarding the Connect.Me Local Terms when they determine whether or not to join the Respect Network.

The first Public Review Version of the Respect Trust Framework was submitted to OIX on 10 May 2011. This Version 1 Beta supersedes the Public Review Version and incorporates the feedback and suggestions received during the public review period. It carries the designation "Beta" because, although it will become the official governing terms for Members of the Respect Network beginning 15 August 2011, it may continue to evolve based on feedback and suggestions received during the Connect.Me and Respect Network beta program. Our intention is to graduate to the full production version by 29 February 2012.

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

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

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 greater confidence that it will be protected 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, 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 Respect 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 Respect 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 (informative) purposes only.

Like the examples, Exhibit C sets forth additional guidance for application of the Respect 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 Respect Principles relate to a subset of current legal authorities. More generally, the individual FIPPs associated with each Respect Principle provide examples of the types of specific duties that are intended to be covered by each Respect Principle, and thereby they collectively help to inform how the Respect 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 identity 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 Promise Principle

***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 Promise 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.

The Promise Principle is directed at causing Members to adopt the duties, in their role as data handlers, to respect other Members' 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 from 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 integrity generally constitutes an intrusion on identity integrity under the Respect Trust Framework. A subset of those Respect Trust Framework intrusions includes 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 represents 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 Respect Network operating under the Respect Trust Framework. For this reason it is referred to with the trademarked name **The Respect Promise™**. This is explicitly defined to mean:

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

The Permission Principle

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 Permission 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 Promise Principle sets up a default duty of non-intrusion (*aka* respect for identity integrity), the Permission 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 the Permission 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 (but not exclusively) 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 Promise Principle, the duties in the Permission 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 Permission Principle’s duty to obtain permission for “all sharing of identity and personal data,” is similar to the duties associated with 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. The 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 Permission 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 Protection Principle

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

The Portability Principle

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

The Portability 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 and share their digital identity and data about them online from a variety of services and in a variety of contexts. The Portability 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 Proof Principle

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 Respect 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 Proof 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 Reputation System™

This section defines the Respect Reputation System that implements the Proof Principle.

Definitions

1. **Member** means any legal person (e.g., individual, commercial, governmental, etc.) that has joined the Respect Network and contractually agreed to the Respect Promise.
2. **Member Account** means the unique account representing a Member as a unique legal person on the Respect Network.
3. **Member Data** means the personal data and identity information controlled by a Member, including data, text, graphics, videos, or other content and materials, for sharing via the Respect Network under the terms of the Respect Trust Framework. For purposes of this definition, the term “controlled by” means sourced from or shared by the Member.
4. **Member-Sourced Data** means Member Data for which the Member is the original source through which such data and information was included in the Respect Network.
5. **Member-Shared Data** means Member Data for which the Member is not the original source through which such data and information was included in the Respect Network, but to which the Member was authorized to provide access or distribute within the Respect Network consistent with the Respect Trust Framework.
6. **Individual Member** means a Member who joins as a natural person representing only himself/herself and not another legal entity.
7. **Organizational Member** means a Member that joins in any legal capacity other than as an Individual Member.
8. **Context** means a uniquely addressable digital representation of a semantic concept with which Members may associate their digital identity. A Context is labeled with a Tag. In addition, a Context may also be labeled with a visual icon or graphic.
9. **Tag** means a human readable semantic label for a Context. Multiple tags that are semantically equivalent, either in the same human language or in different human languages, may be assigned to the same Context.
10. **Community** means the set of Members and Member Data associated with a specific Context.
11. **Vouch** means a signal of positive reputation in a specific Context made by one Member about another Member.
12. **Complaint** means a signal of negative reputation in any Context made by one Member about another Member.
13. **Voucher** means the Member making a Vouch.
14. **Complainant** means the Member making a Complaint.
15. **Recipient** means the Member that is the subject of a Vouch or a Complaint.
16. **Trust Level** means an indicator of the level of expectation that a Member will abide by his/her Respect Promise. Each Trust Level has a set of requirements a Member must meet to achieve that Trust Level as defined in the Trust Levels section below.
17. **Trust Anchor** means the highest Trust Level as defined in the Trust Levels section below.

18. **Trust Anchor Context** means the special Context in which Trust Anchors may Vouch for other Recipients to enable them to achieve Trust Anchor status.
19. **Reputation Graph** is the metadata describing a Member that includes the Member's Contexts, Communities, Vouches and Complaints given and received, and Trust Level.
20. **Profile** is the specific view of Member Data and the associated Reputation Graph available to other Members in a specific Context, or to the public if the Profile is public.
21. **Persona** is a representation of a Member's digital identity controlled by that Member.
22. **Dashboard** is the interface Connect.Me provides Members for setting preferences and sending and receiving communications through the Respect Network.

Trust Levels

1. This version of the Respect Trust Framework explicitly defines four Trust Levels for Individual Members only. In future versions additional Trust Levels may be defined as needed to further the purpose and principles of the Respect Trust Framework.
2. A Member's Reputation Graph is automatically assigned a Trust Level as soon as the Member meets the requirements of that Trust Level. Conversely, as soon as a Member no longer meets the requirements of a Trust Level, the Member shall automatically be assigned to the next lower Trust Level for which the Member meets all the requirements.
3. A Member's Trust Level assignment may also be changed by resolution of a Complaint as defined in the Complaint section below.
4. The lowest Trust Level is **Unverified**. This is the minimum Trust Level that applies to all Individual Members. The requirements to become an Unverified Member are: a) the Member must successfully complete registration with the network, and b) the Member must contractually agree to the Respect Promise.
5. The next higher Trust Level is **Verified**. The requirement to become a Verified Member is that an Individual Member must: a) verify their ownership of one or more external accounts and/or personal data attributes that meet the requirements published by Connect.Me at <http://connect.me/c/verification>, b) have given at least 10 Vouches to other Individual Members, and c) have received at least 10 Vouches from other Individual Members (the "10/10 Rule").
6. The next higher Trust Level is **Trusted**. The requirement to become a Trusted Member are that an Individual Member must: a) be a Verified Member, b) have given at least 25 Vouches to other Individual Members, and b) have received at least 25 Vouches from other Individual Members whose trust level is Verified or higher (the "25/25 Rule").
7. The highest Trust Level is **Trust Anchor**. Unless a Member is a Founding Trust Anchor (below), the requirements to become a Trust Anchor are that an Individual Member must: a) be a Trusted Member, and b) have received at least three Vouches in the Trust Anchor Context from another Trust Anchor.
8. To bootstrap the population of Trust Anchors, Connect.Me may appoint **Founding Trust Anchors**. The requirements to become a Founding Trust Anchor are: a) the Member must be known to a representative or delegate of Connect.Me and have agreed to become a Founding Trust Anchor via contact (in person or online) with such representative or delegate, and b) the Member must become a Trusted Member.

9. Connect.Me may prospectively and uniformly adjust the number of Vouches required of Members to become a Verified Member, Trusted Member, or Trust Anchor without requiring a new version of the Respect Trust Framework if such adjustment will, in Connect.Me's judgment, further the purpose of the Respect Trust Framework.

Accountability Rules

1. **One-Person-One-Account.** Every Member agrees to register and maintain one and only one Member Account. Every Member understands and acknowledges that maintaining the One-Person-One-Account Rule is essential to maintaining the integrity of the Respect Network, the Respect Reputation System, and the Respect Trust Framework.
2. **Accountability for Vouches.** Every Member agrees that when the Member Vouches for a Recipient, the Member is representing that: a) the Member believes that the Recipient's Member Account represents the true legal person the Member believes the Recipient to be; b) the Member has no knowledge of the Recipient having more than one Member Account on the Respect Network at the time of the Vouch; and c) the Member has no reason to believe that the Recipient is attempting to game or subvert the Respect Reputation System, or is otherwise violating the purpose, principles, or rules of the Respect Trust Framework.
3. **Accountability for Trust Anchor Vouches.** Every Trust Anchor agrees that a Vouch in the Trust Anchor Context means that the Voucher personally knows the Recipient and has good reason to believe that the Recipient will honor and abide by the Respect Promise.
4. **Accountability for Personas.** Every Member agrees that when the Respect Network incorporates support for anonymous or pseudonymous Personas, the single Member Account responsible for those Personas will be ultimately responsible for issuing and accepting Vouches, issuing and processing Complaints, joining Communities, managing Profiles, sharing Member Data, voting for Amendments to the Respect Trust Framework, and any other action that represents the Member's official activity through a Persona on the Respect Network.
5. **Accountability for Credentials.** Following the Protection Principle, every Member agrees to keep his/her Member Account authentication credentials private; to maintain reasonable security over these credentials; and to promptly notify Connect.Me if the Member has reason to believe the credentials have been leaked, stolen, or otherwise compromised.
6. **No Abusive Vouching.** Every Member agrees not use a Vouch for any other purpose than to send an honest signal of positive reputation about a Recipient. Abusive vouching includes using a Vouch to attempt to send a signal of negative reputation by Vouching in a Context intended to insult, demean, degrade, or otherwise harm the reputation of a Recipient; using a Vouch to solicit or otherwise capture the attention of the Recipient for such other purpose; or using the Vouching system to otherwise interfere with Recipient's usage and enjoyment of the Respect Network.

Vouching Rules

1. Any Member may Vouch for any other Member in any Context.
2. All Vouches are public for both the Voucher and the Recipient.
3. Recipients may control what Contexts appear in their public Persona. Communities may control what Contexts are required to appear in a Persona used within a Community.

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.

Complaint Rules

1. Any Member whose Trust Level is Verified or higher may submit a Complaint with regard to any other Member whom the Complainant believes has violated the purpose, principles, or rules of the Respect Trust Framework.
2. The Complaint must state, in free form text and/or by selection from a user interface option, the nature of the violation.
3. Once a Complaint in proper form is submitted to Connect.Me, it shall be automatically posted to the Reputation Graph of the Complainant, but not to the Reputation Graph of the Recipient unless and until the Complaint is upheld. In addition, the Recipient shall be automatically notified of the Complaint via the Recipient's Connect.Me Dashboard.
4. The Complaint shall then be automatically submitted by Connect.Me to one or more Trust Anchors for resolution (individually "Panelists" and collectively the "Panel"). A Panelist who has Vouched for either the Complainant or Recipient shall be automatically disqualified from that Panel and replaced with another Panelist.
5. The Panel shall have the option at any time during its deliberations to request that additional Trust Anchors be assigned as Panelists. If the existing Panel agrees, Connect.Me shall automatically assign the number of additional Panelists agreed by the existing Panel.
6. The Panel shall have sole authority to request additional information from either the Complainant or Recipient as needed to resolve the Complaint. Complainants and Recipients agree to cooperate with the Panel so as to expeditiously resolve a Complaint.
7. All communications regarding the Complaint shall take place via communications channels authorized and agreed to by the parties involved. If no other channel is authorized, communications shall take place via the parties' Connect.Me Dashboards.
8. All communications regarding resolution of a Complaint, but not the final decision of the Panel, shall be treated as confidential by all parties to this Complaint process. Members agree that Connect.Me shall have access to such communications to help Connect.Me research methods for improving the Complaint process and better serve Members.
9. The Panel shall work as diligently and expeditiously as possible to reach one of four conclusions regarding a Complaint: a) dismissed, b) resolved c) upheld, d) denied. The Panel may reach a conclusion at any point in the process based on the evidence before the Panel and the communications or lack thereof from the Complainant and Recipient. If the Panel consists of more than one Panelist, the decision shall be made by simple majority.
10. The Complaint shall be dismissed if the Panel concludes that it falls outside the scope of the Respect Trust Framework. The Complaint process is solely intended to address actions by Members 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 in this document, including but not limited to monetary and injunctive relief, are outside the scope of the Complaint process and will not be considered. If a Complaint is dismissed, it shall be promptly removed from the Reputation Graph of the Complainant.
11. A Complaint shall be resolved if, either through the intervention of the Panel or by the Complainant's and Recipient's own independent means, both the Complainant and

Recipient notify the Panel that the Complaint has been resolved. If a Complaint is resolved, it shall be promptly removed from the Reputation Graph of the Complainant.

12. A Complaint shall be upheld if the Panel concludes that the Recipient has violated the Respect Trust Framework. If the Complaint is upheld, the Panel shall have sole authority to decide: a) for what period the Complaint shall become part of the public Reputation Graph of the Recipient, b) what annotation about the nature and severity of the Complaint shall be included, if any, c) what adjustment shall be made to the Trust Level of the Recipient, if any, and d) for how long such adjustment shall remain in force.
13. A Complaint shall be denied if the Panel concludes that the Recipient did not violate the Respect Trust Framework. If a Complaint is denied, it shall be promptly removed from the Reputation Graph of the Complainant. Furthermore, the Panel shall decide if the Complainant did not have legitimate grounds for submitting the Complaint (“Unfair Complaint”). If the Panel concludes the Complaint was an Unfair Complaint, the Panel shall have sole authority to decide: a) for what period the Unfair Complaint shall become part of the public Reputation Graph of the Complainant, b) what annotation about the nature of the Unfair Complaint shall be included, if any, including whether the available evidence suggested that the Complainant was submitted to cause reputational harm to the Recipient, c) what adjustment shall be made to the Trust Level of the Complainant, if any, and d) for how long such adjustment shall remain in force.

Local Terms

The Respect Trust Framework is intended to establish a set of terms that apply globally to all relationships and exchanges of personal data that take place between Members through the Respect Network (“Global Terms”). For some relationships or exchanges these Global Terms may be sufficient. For other relationships or exchanges these Global Terms may need to be supplemented by other terms specific to a particular relationship or exchange (“Local Terms”). Examples of Local Terms include terms-of-service agreements, localized privacy policies, specialized security policies, and other context-specific policies. Local Terms may be part of Plug-In Trust Frameworks (see below), or they may be more limited, stand-alone sets of Local Terms.

By joining the Respect Network, a Member agrees that the Local Terms the Member requires for any relationship or exchange with other Members will not conflict with, or require an alternative interpretation of, the Global Terms of the Respect Trust Framework. (This rule also applies to Connect.Me itself, as explained in the Status section above.)

Plug-In Trust Frameworks

The Respect Trust Framework is intended to provide a global set of principles and rules for protection of identity and personal data on a digital trust network. Groups of Members may desire to develop more specific sets of principles and rules applicable 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 current version of the Respect Trust Framework.
2. It must not define principles or rules in conflict with, or requiring an alternate interpretation of, the principles or rules defined in the Respect Trust Framework.

Versioning and Amendments

Given that the purpose of the Respect Trust Framework is to engender trust among Members of a trust network, it is of utmost importance that the Members be able to rely on the integrity and stability of the trust framework itself. For this reason, any amendments to the Respect Trust Framework after February 29, 2012 may only be approved by the Members of the Respect Network according to the following rules.

1. All Members shall receive formal notice of the vote (“Voting Notice”) from Connect.Me via an electronic message delivered to their Dashboard including a link to an electronic ballot with relevant information about the proposed amendment. This is the only way that an amendment to the Respect Trust Framework may be initiated.
2. All Trust Anchors as of the time Voting Notice is issued shall be eligible to vote on the amendment. No other Members are eligible to vote.
3. The Voting Notice shall be made at least thirty calendar days prior to the deadline by which a ballot must be submitted (“Voting Deadline”) to permit Members time to read, study, and debate the amendment.
4. Each Trust Anchor shall be allocated 100 votes.
5. A Trust Anchor 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. Proxies will only be recognized if established through official Connect.Me voting proxy processes.
6. There is no required quorum.
7. An amendment shall pass if, after passage of the Voting Deadline, it has received 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 amended version shall be effective 30 days after the announcement.

Copyrights and Trademarks

The Respect Trust Framework is copyright 2011 Respect Network Corporation.

Connect.Me™, Respect Network™, Respect Trust Framework™, Respect Reputation System™, and Respect Promise™ are trademarks of Respect Network Corporation.

Respect Network Corporation
548 Market St #98486, San Francisco, CA 94104, USA

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.

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
(For the full text of each principle, see
http://publications.apec.org/publication-detail.php?pub_id=390)

A-1	PREVENTING HARM
A-2	NOTICE
A-3	COLLECTION LIMITATION
A-4	USES OF PERSONAL INFORMATION
A-5	CHOICE
A-6	INTEGRITY OF PERSONAL INFORMATION
A-7	SECURITY SAFEGUARDS
A-8	ACCESS AND CORRECTION
A-9	ACCOUNTABILITY

GSMA (For the full text of each principle, see http://www.gsmworld.com/documents/GSMA_Privacy_Principles_UPDATED.pdf)	
GSMA-1	OPENNESS, TRANSPARENCY AND NOTICE
GSMA-2	PURPOSE AND USE
GSMA-3	USER CHOICE AND CONTROL
GSMA-4	DATA MINIMIZATION AND RETENTION
GSMA-5	RESPECT USER RIGHTS
GSMA-6	SECURITY
GSMA-7	EDUCATION
GSMA-8	CHILDREN AND ADOLESCENTS
GSMA-9	ACCOUNTABILITY AND ENFORCEMENT