

Exhibit 4

Data Action Survey Tool

(formerly the “Verbs Taxonomy”)

**Draft 1.2
February 10, 2011**

Discussion and Development Materials

of the

OIX Advisory Committee

and the

OIX Legal Policy Committee

Notes to user:

This tool has been prepared for use by the OIX Advisory Committee and the OIX Legal Policy Committee and by any other parties involved in online and telecommunications data/identity system legal standardization, risk and liability analysis, and trust framework, legislation and contract development work.

The tool is made available by OIX under a creative commons license (with attribution), so that it is broadly available to all interested parties.

These materials and the online or other discussions that use or refer to these materials are not intended to provide legal advice. They are only intended for use as a reference tool in the consideration and discussion of issues associated with the design, development and deployment of data and information resource management systems and online and telecommunications identity management systems. Parties should seek the advice of legal counsel in each relevant jurisdiction before implementing any business or personal decision that involves the establishment of legal duties, the management of legal risks or the potential for legal liability.

The online functionality at www.openidentityexchange.org is made available for public use pursuant to the terms of use [link] posted on the OIX website.

If you are not familiar with the use of this Tool, please see the “User Guide” (see table of contents).

Notes and expanded discussion relating to this tool (to be considered for inclusion in the OIX Risk Wiki) are available at [Insert reference to appendix].

The online functionality at www.openidentityexchange.org based on this tool is made available for public use pursuant to the terms of use [TOU link here] posted on the OIX website.

[OIX Administrative NOTE: The foregoing reference to a TOU is needed to collect the necessary rights from, and make needed disclosures to, persons posting content to the OIX Risk WIKI and other online tools and programs in order to accumulate and share their contributions with other stakeholders through the tool. It is anticipated that the public use of the online WIKI tool will generate postings, the continued accumulation of which will constitute a “community-generated” and “community-maintained” “virtual discussion” that will keep the legal analysis dynamically current as an issue-spotting resource to inform the collective analysis and discussion, and to help identify system-relevant future modifications to the Listing information requirements for the OIX listing service and other OIX programs. We should explore designing the WIKI so that it can most easily track alternative analyses for forking (and recombining) issues (such as, for example, when an identical transactions are entered into, subject to two different countries’ laws.)]

Introduction

This Data Action Survey Tool is intended to be used with the OIX Risk Wiki and the OIX Data Flow Mapping Tool. Together, these tools can assist both:

- (i) Users of existing networked data/identity systems: Relying parties, data subjects (and the data/identity system assessors and auditors on which they rely), and other system users in understanding and evaluating the data flows (and related risks and available solutions) in existing data/identity systems, and
- (ii) Developers of new networked data/identity systems: Data/identity system “Tools and Rules” designers and developers (i.e., technologists, policy and legal developers), and entities involved in deploying systems, in configuring data flows in future systems that are being developed, or evaluated for modification.

A focus on real-world “data actions”

The Tools all focus on “actions” taken with respect to data, such as “collection of data,” “transfer of data,” and “disposal of data.” The Tools help to “unpack” system data actions so that each can be examined separately and then in combination in a particular system and context. Each of these actions is relevant for both technical and legal purposes.

Technical specifications are built around specific data actions. For example, the technology solutions associated with security are different for the data action of “holding data” (such as firewalls, encryption, etc.), than they are for “disposing of data” (degaussing, overwriting, etc.).

Similarly, legal analysis is guided by specific data actions. For example, in the U.S., a person engaging in the action of “collection of data” in the financial context is subject to statutory and regulatory legal duties (which together act like a legal “specification”) under the Gramm Leach Bliley Act to provide prior notice including the presentation of a privacy policy and the ability of the data subject to “opt out” of receiving third party marketing communications.

By contrast, there is no legal duty to give notice or to present a privacy policy or “opt out” when data is disposed of by a business, but some states, such as California, impose a legal duty in the form of a legal “standard of care” to dispose of the data by “(1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.”

Notably, “legal specifications” can also take the form of contractual legal duties established under broadly adopted standardized agreements used in various commercial markets, social communities and political governance structures. For example, a retailer (which has a role similar to that of a “relying party”) engaging in the action of “collection of data” in the credit card context is subject to contractual duties (which also act like a legal “specification”) under PCI-DSS to engage in specific card acceptance rituals (that are intended to maintain payment card system integrity).

The specific types and natures of data actions taken by different stakeholders within a particular system in a particular context drive configuration of both technical specifications and legal standard terms. Standard systems and broad data/identity system infrastructure can be built from the “normalization” of data actions that are regularly engaged in across system contexts and user groups. The Trust Framework is the place in which the relevant technology Tools and legal Rules parameters for a given system are documented.

Thus, the focus on data actions enables the production of hybrid Trust Frameworks that simultaneously configure both technology “Tools” and legal “Rules” as the virtual “plumbing” for online data/identity systems.

As evidenced by the examples above, the reasons for having different technical and legal requirements for different data actions are obvious since each is designed to accomplish a particular result as part of the overall data “system” functionality. The focus on data actions in networked systems can provide the common foundation for a shared analysis of how data resources are used by different user groups (through their respective data actions) in the commercial, social and political contexts, which can enable the mutual exploration and accomplishment of consensus-based data resource management solutions which have risk (and cost) reduction and market expansion benefits to all stakeholders.

The OIX “I_AM” process identifies duties to address privacy, security and liability issues

The Risk Wiki provides a structure to evaluate the various identified data actions. It applies a three step process through which data actions, background law, and stakeholder needs are brought together in the analysis to inform the identification of duties, the analysis of risks and the management of liabilities. Such “Identification,” “Analysis” and “Management” is generally called the OIX “I_AM” process.

The OIX “I_AM” process is intended to assist in the analysis and design of legal structures to address secure online transaction/identity management (SOT/IDM) duties, risks and liabilities. Please see the notes accompanying the OIX Risk Wiki at [link] for explanation of the “I_AM” process and a fuller description of the stakeholder rights and obligations relating to the SOT/IDM context.

In the Risk Wiki, the I_AM process is applied to help in the evaluation of duties, risks and liabilities with respect to the 9 types of SOT/IDM Data Actions that take place in a typical third party authenticated SOT/IDM transaction.

What are categories of data actions?

Each of these Data Actions involves a specific set of sub actions taken with respect to a particular piece of data or information by a particular person. These sub-action “verbs” include

Collection of data,
Access to data

sharing data with others,
holding data,
use of data, and
disposal of data¹

Each “verb” above describes a general category of data action. For each, this attachment provides:

1. A “working” definition (this is not a dictionary definition, but a functional definition meant to be applied in the context of actions involving data and information, and informed by applicable U.S. law).
2. A list of questions directed at identifying additional variables that can inform the analysis of legal duties, risks and liabilities, and which can also provide a prompt for Trust Communities and Trust Framework developers in the process of considering what to include in their respective Trust Frameworks.

PLEASE NOTE: Where this tool is used to review or audit existing data flow systems, detailed answers to the questions in this survey tool can reveal detailed and sensitive information about data and information systems and flows in an organization or made by an individual. It is recommended that you **DO NOT POST SPECIFIC RESPONSES ABOUT CONFIDENTIAL OR SENSITIVE ELEMENTS OF YOUR DATA AND INFORMATION SYSTEMS ON THE RISK WIKI**. If your in-house analysis reveals an interesting or helpful issue that would benefit the online identity community, you are invited to consider posting it as a generic comment to the Risk WIKI.

¹ Note that there are other “data action verbs” that are potentially important in different contexts that might be distinguished from the above. These include actions such as those indicated by current French privacy legislation to constitute “Processing of personal information” such as “obtaining, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.” Of these, it is primarily “modification” that is not yet separately referenced in the current tool (but is covered under the general category of “use.”) As the concepts of “privacy” and “data security” continue to be developed toward more comprehensive concepts of “networked-identity integrity,” additional actions of third parties that constitute potential intrusions (and that subset of legally-cognizable and legally actionable intrusions) on such newly discerned “integrity” will continue to be identified. This and other OIX tools are designed to easily accommodate the addition of new and modified actions that are deemed to have legal consequences in a given jurisdiction or commercial, social or governmental context. In this way, the tool can “scale” with the scope of activities with respect to which data is transferred in networked systems.

Collection of Data

Working Definition:

"Collect" means to receive from someone outside of the collecting Stakeholder or its affiliates, whether an individual data subject or a third party.

Survey Questions:

- 1. *Collected From Data Subject?***
If the collection of data takes place over the Stakeholder website, assume that it will constitute a "transfer" and Stakeholder should also consider the relevant "transfer" questions. Also consider "transfer" questions if collect data by mail or call or otherwise send data from a foreign country
- 2. *Are Data Subjects Stakeholder employees?***
Employee information may enjoy special status.
- 3. *Points of collection of data?***
Consider alternative points of collection by a single entity, since each may have particular requirements. Consider registration information, post-registration corrections of data, third party data sources.
- 4. *Collect From Third Party?***
"Third Party" here means anyone other than the subject of the data collected. Consider data acquired from public databases (and TOUs of same), online logs and tracking, purchase of lists, [note for Verb Taxonomy development] - create a list of databases and third parties used by Stakeholder, such as consumer reporting agencies, etc. for use here].
- 5. *Is there a contract, privacy policy or law that governs this collection?***
Consider sources of restrictions on collection or use (such as a privacy policy or contract). In audit situation, acquire a copy of the document. Where there is no TOU, consider alternative contractual and statutory responsibilities relating to collection of that data.
- 6. *Type of data subject***
Consider the various special categories of data subject under relevant data laws, such as: Current Personnel, Former Personnel, Job Applicants, Shareholders, Vendors/Subcontractors, Existing Customers, Prospective Customers, underage individuals, employee benefits plan beneficiaries.
- 7. *Purpose of collection?***
Consider intentions and purposes of collection. Be specific. Consider whether the purpose could be achieved without collecting the data.
- 8. *Data subject residence country?***

Consider country/state (province) of data subject

9. ***Media and Manner in which data collected?***

Consider alternative media over which data providing identity information could be delivered including e-mail, postal mail, IM, from a website, fax, phone (landline, cell, VOIP), VRI (Virtual Reality Interfaces), file transfer, system to system web service communication, removable media.

10. ***Are measures taken to verify any data?***

Are third parties such as authentication services or consumer reporting agencies used to verify any information? Consider verification of disability claims, credit cards, background checks.

Access to Data

Working Definition:

"Access" means to receive or have access to from a source *inside of* an entity (as opposed to individual) Stakeholder.

Survey Questions:

1. ***To your knowledge, who can access this data?***
Consider access by data subject, Stakeholder personnel, Vendors or contractors, accountants, lawyers, insurance companies, other. Consider related questions re: purpose of access.
2. ***Within Stakeholder, where does the data reside when accessed?***
Consider servers, files, interoffice mail, joint data bases, other paper, e-mail, within Stakeholder and affiliates, data accessible by links, Stakeholder internal reports.
3. ***In what country is the data held?***
Consider data transfer issues associated with intracompany, international transfers (e.g., is in-house remote access a "transfer" under applicable law)
4. ***From what countries is the data accessible?***
Consider jurisdictions in which data requester is located.
5. ***Ask: "Do you need access to this data to do your job?"***
The purpose of this question is to identify data that is received by a person, but not needed to do job so that "least data" principles can be considered.
6. ***Do you have authorization to access this data?***
Trace specific authorizations (including formal legal authorizations where applicable) for access to any regulated or sensitive data.
7. ***Who can create, edit, add or delete data?***
Consider if one or more of the Data subject, Stakeholder personnel, Vendors or contractors, accountants, lawyers, insurance companies, other can engage in data modification. Consider question of whether data subject is provided notice of changes made.
8. ***Can data subject edit, add or delete data?***
Consider system implications of various responses.
9. ***What security measures limit access to this data?***
Consider what security controls are in place for data access. For example:
No security controls
Physical controls (such as locked file cabinet and access controlled room),

Administrative controls (such as access permitted with permission of database manager, access permitted only with data subject consent, access permitted on need to know basis, NDA requirement,

Electronic controls (such as user ID and password, high security controls such as biometrics), electronic intruder detection, secure servers, firewalls, encryption, virus protection, smart cards, access cards, virtual network, electronic signatures, dedicated lines

10. ***Is access to database logged?***

This question should be posed to tech person at Stakeholder.

11. ***Are changes to database logged?***

This question should be posed to a tech person at Stakeholder.

12. ***Is there a policy for reporting or responding to unauthorized access to data?***

13. ***Is there data breach response policy for this data?***

Sharing Data with Others

Working Definition:

"Share with others" means to grant or give access to others, whether inside or outside of Stakeholder. This includes posting on a website or sharepoint, transfer of files, granting of access to files, display within an application viewer, printing out a copy for another. Where "access" is the "action" of data receipt, "share with others" is the opposite action, a form of data "giving."

Survey Questions:

1. *Is there ever a transfer/disclosure to Stakeholder employee or Stakeholder affiliate?*
Affiliate means a related entity in the Stakeholder family.
2. *Is there ever a transfer/disclosure to 3rd party outside Stakeholder?*
Consider different third parties, including agents, service providers, processors (e.g. payroll or credit card), banks, mailing houses, marketers, governmental authorities, Data subject, Stakeholder personnel, accountants, lawyers, vendors contractors, insurance companies, etc. Consider the purposes of all such transfers, and whether they are necessary.
3. *Are all transfer of this data within the U.S.?*
Consider country of origin and source of sharing and implications of same..
4. *How is the transfer made?*
Consider various mechanisms for transfer, such as interoffice mail, e-mail, postal mail, courier, common access to database, fax, removable physical media, and physical aspects of network over which made, i.e., cell, Bluetooth, public wifi, etc.).
5. *Is transfer or disclosure recorded?*

Holding Data

Working Definition:

"Hold" means to store data for any period longer than the time necessary for its initial use.

Survey Questions:

1. ***What is the purpose of retention or storage?***
Consider various purposes such as audit, customer care, financial records, general administration, marketing.
2. ***Length of data retention period?***
Be specific on length of time specified in policies, and actual retention practices. Consider if any data is held indefinitely. Consider if there is a relevant external period to reference (such as statute of limitations.). If any response is made other than "indefinitely," consider the "disposal" questions for all relevant data types.
3. ***Where is data stored? (database, file name, server, drive location)***
The purpose of this question is to help Stakeholder actually locate data and identify needed access controls.
4. ***Physical location of data receptacle?***
5. ***Is data stored by third party?***
6. ***Is data stored as paper, electronic, optical or multiple media?***
7. ***Is data stored on mobile or removable device or media?***
Consider such devices as paper files, servers, hard disk drives, floppy drives, zip drives, tapes, CD, network, laptops, thumb drives, mobiles, cell phones, cameras (including cell phone cameras), Ipods, other.
8. ***Are copies made of data?***
Consider photocopies, handwritten, electronic copies, scanner. Consider whether the purpose of making the copy could be achieved without making a copy (least data principle).
9. ***What security is used for data storage?***
Consider the variety of physical, technological and administrative techniques, such as encryption, password protection, redaction, locking cabinets, and other access controls.
10. ***Who can access stored data?***
Consider list of possible persons with access such as employees, administrators, third party service providers, etc.

11. *Who is in charge of data?*

Use of Data

Working Definition:

"Use" means to do anything with data other than holding it or transferring it.

Survey Questions:

1. *For what is data used?*

Consider any possible business, administrative or other uses, for example: contacting data subjects, research, accounting, HR, marketing, internal reporting, recruiting, legal process, Stakeholder investigations/lawsuits. Note that the practices revealed by answers to this question should be compared to terms of any privacy policy or contract identified in the responses to the "collection" question involving privacy policies.

2. *Do you de-identify the data?*

Consider the disposition of the original data and information where use "de-identified" data.

3. *Is a copy made prior to or as part of use?*

Consider where that copy is stored.

4. *Is data combined with other data?*

"Combined" includes merged, correlated, aggregated or otherwise combined with any other database. Is the combination reversible, i.e., if Stakeholder had a legal obligation to destroy the data, could it do so without destroying the new database?

Disposal of Data

Working Definition:

"Dispose of" means any act to delete, get rid of, or eliminate data or information in any form.

Survey Questions:

1. *Form of data disposed of?*

Consider form of data at time of disposal such as paper, electronic, fax, external drive or disk, internal device memory, file (where "disposal" consists of pressing "delete" button), other. For each particular media, consider appropriate follow up questions to address special requirement of local (such as state) data disposal laws for personal information..

2. *Has the data ever had another form?*

Consider what has happened to any of the same data or information other than that stored in the format being disposed of.

3. *Who carried out the disposal?*

Consider whether the disposal was carried out by an Stakeholder employee or a third party and contractual arrangements with such party.

4. *Mechanism of disposal?*

Consider physical mechanisms of disposal used, including for example: wastebasket, recycling bin, shredding bin, destruction of media, deliver to professional disposal service, etc. .For certain data types consider whether local law requires special steps to be taken such as formal policies, due diligence on the disposer and application of particular technological steps to assure destruction of data.