

Exhibit 7

**Fair Information Practice Principles (FIPPs)
Comparison Tool**

**Draft 1.2
February 11, 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 Appendix 2.

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.)]

FIPP Comparison Tool

Table of Contents

Cover page	
Notes to user	
Table of Contents	
I. Data Collection	
1. Data Handler Openness.....	
2. Data Handler Accountability.....	
3. Notice/Identify Purposes/Consent.....	
4. Limits on Collection/Least Data Principle.....	
a. What data collected.....	
b. How collected.....	
c. What and how collected.....	
II. Data Processing	
5. Data Security.....	
6. Use Limitations.....	
a. Limit use.....	
b. Limit disclosure.....	
c. Limit retention.....	
7. Data Accuracy.....	
8. Access to Data / Right to Amend.....	
a. Access only.....	
b. Amendment only.....	
c. Access and amendment.....	
III. Data Distribution	
Disclosure Limitations – See section 6.b. in Part II.	
IV. Other	
9. Public Interest Exceptions.....	

10. Other.....

V. OIX FIPPs Comparison Tool User Guide.....

Appendix 1 – List of FIPPs.....

Appendix 2 - Legal Review Notes on the FIPPs Tool
for inclusion in OIX Risk Wiki.....

OIX FIPPS COMPARISON TOOL

Part I – Data Collection

1. Data Handler Openness

There must be no personal-data record-keeping systems whose very existence is secret. (HEW 1)

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. (The Openness Principle) (PPSC; 1)

*[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; Art. 8.a. Additional safeguards for the data subject)

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; Openness Principle)

Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection; (EU; Section 38)

Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. (Canada MC; section 8)

Transparency: Organizations should be transparent and provide notice to the individual regarding collection, use, dissemination, and maintenance of personally identifiable information (PII). (Draft NSTIC)

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. (Draft NSTIC)

Part I – Data Collection

1. Data Handler Openness (continued)

Open reporting and publication. OITF Providers must produce periodic reports on the operation and governance of the trust framework. They must ensure that a web site devoted to the OITF provides easy and timely access to (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. OITF Providers must ensure that all parties to agreements under the OITF have visibility into who is participating in it and in what capacity. (OITF WP)

Anti-circumvention and open disclosure. OITF participants must not be party to any side agreements that compromise the integrity of commitments under the trust framework. 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. OITF Providers and assessors must disclose all their agreements and the terms of those agreements. (OITF WP)

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 WP)

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 WP)

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 WP)

Part I – Data Collection

2. Data Handler Accountability

A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems. (The Accountability Principle) (PPSC; Section 8)

Accountability Principle: A data controller should be accountable for complying with measures, which give effect to the principles stated above. (OECD)

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 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. (Canada MC; Section 1)

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. (Canada MC; Section 10)

Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements. (Draft NSTIC)

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. 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. (OITF WP)

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 WP)

Part I – Data Collection

3. Notice/Identify Purposes/Consent

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)

Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). (DHS 1)

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 1)

Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party; (EU; Section 39)

Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. (Canada MC; Section 2)

Consent: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. (Canada MC; Section 3)

Notice - Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (*e.g.*, directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site. (FTC)

Opt In – Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction. (ICAM; Section 3.3, 2.a.)

Part I – Data Collection

3. Notice/Identify Purposes/Consent

Adequate Notice – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process. (ICAM; Section 3.3, 2.d.)

Transparency: Organizations should be transparent and provide notice to the individual regarding collection, use, dissemination, and maintenance of personally identifiable information (PII). (Draft NSTIC)

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. (Draft NSTIC)

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. (Draft NSTIC)

Part I – Data Collection

4. Limits on Collection/Least Data Principle

4.a. What data is collected?

The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose. (COP 1; Section 3)

[Personal data undergoing automatic processing shall be:] adequate, relevant and not excessive in relation to the purposes for which they are stored; (COE; Article 5.c. Quality of data)

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)

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 1)

*[Personal files shall be set up and kept in such a way that no undue encroachment upon the personal privacy of a registered person occurs. In this respect special attention shall be paid to the following points:]*that no other particulars are recorded than are in accordance with the purpose of the file (Sweden; Section 4)

*[Personal files shall be set up and kept in such a way that no undue encroachment upon the personal privacy of a registered person occurs. In this respect special attention shall be paid to the following points:]*that no particulars are collected, disseminated or used other than in accordance with the purpose of the file or with the provisions of law or other statute or with the permission of the registered person) (Sweden; Section 3)

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). (Draft NSTIC)

Part I – Data Collection

4. Limits on Collection/Least Data Principle (continued)

4.b. How is data collected?

*[Personal data undergoing automatic processing shall be:]*obtained and processed fairly and lawfully; (COE; Article 5.a. - *Quality of data*)

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)

Part I – Data Collection

4. Limits on Collection/Least Data Principle (continued)

4.c. What data is collected and how is data collected?

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. (The Collection Limitation Principle) (PPSC; Section 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. (Canada MC; Section 4)

Part II – Data Processing

5. Data Security

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 of the data. (HEW 1)

Access to information should be confined to those authorized to have it for the purpose for which it was supplied. (COP 1; Section 1)

The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information. (COP 1; Section 6)

A monitoring system should be provided to facilitate the detection of any violation of the security system. (COP 1; Section 7)

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. (COE; Article 7)

Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information. (COE; Art. 15, 2.)

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)

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 1)

Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional; (EU; Section 42)

Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. (Canada MC; Section 7)

Security - Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers. (FTC)

Part II – Data Processing

5. Data Security (continued)

[Personal files shall be set up and kept in such a way that no undue encroachment upon the personal privacy of a registered person occurs. In this respect special attention shall be paid to the following points:]that the particulars in the file are protected against unintentional or unlawful destruction or) against unlawful alteration or dissemination (Sweden)

Termination – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII. (ICAM; Section 3.3, 2.f.)

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. (Draft NSTIC)

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 WP)

Part II – Data Processing

6. Use Limitations

Please note that Use and Disclosure limitations are included in the “Processing” category since some of the FIPPs versions combine suggested limits on use and disclosure. Those FIPPs that limit disclosure (whether or not they also limit use) are also listed under the Category III “Dissemination”

a. Limit use

Information should be regarded as held for a specific purpose and not to be used, without appropriate authorization, for other purposes. (COP 1; Section 1)

There shall be limits on the internal uses of information about an individual within a record-keeping organization. (The Use Limitation Principle) (PPSC; Section 5)

[Personal data undergoing automatic processing shall be:] stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (COE; Article 5.b. - Quality of data)

An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance. (COE; Article 15.1.)

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 1)

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. (Canada MC; Section 5)

Choice - Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (*e.g.*, to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities). (FTC; Section 2)

*[Personal files shall be set up and kept in such a way that no undue encroachment upon the personal privacy of a registered person occurs. In this respect special attention shall be paid to the following points:]*that the file is kept for a specific purpose (Sweden)

Activity Tracking – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than

federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002. (ICAM Section 3.3, 2.c.)

Part II – Data Processing

6. Use, Disclosure and Retention Limitations

a. Limit use

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. (Draft NSTIC)

6. Use, Disclosure and Retention Limitations (continued)

b. Limit disclosure

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 1)

There shall be limits on the external disclosures of information about an individual a record-keeping organization may make. (The Disclosure Limitation Principle) (PPSC; Section 6)

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. (The Information Management Principle) (PPSC; Section 7)

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law. (OECD)

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 1)

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. (Canada MC; Section 5)

Choice - Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (*e.g.*, to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities). (FTC; Section 2)

Minimalism – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002. (ICAM; Section 3.3, 2.b.)

Part II – Data Processing

6. Use, Disclosure and Retention Limitations (continued)

b. Limit disclosure (continued)

Activity Tracking – Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002. (ICAM; Section 3.3, 2.c.)

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. (Draft NSTIC)

Part II – Data Processing

6. Use, Disclosure and Retention Limitations (continued)

c. Limit retention

In the design of information systems, periods should be specified beyond which the information should not be retained. (COP 1; Section 8)

[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; *Article 5.e. - Quality of data -*)

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 1)

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). (Draft NSTIC)

Part II – Data Processing

7. Data Accuracy

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 of the data. (HEW 1)

Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information. (COP 1; Section 9)

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. (The Information Management Principle) (PPSC; Section 7)

[Personal data undergoing automatic processing shall be:] accurate and, where necessary, kept up to date; (COE; Article 5.d. - Quality of data)

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)

Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. (DHS 1)

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. (Canada MC; Section 6)

Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. (Draft NSTIC)

Part II – Data Processing

8. Access to Data / Right to Amend

a. Access only

There must be a way for an individual to find out what information about him is in a record and how it is used. (HEW 1)

There should be arrangements whereby the subject could be told about the information held concerning him. (COP 1; Section 5)

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. (The Individual Access Principle) (PPSC; Section 2)

[*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; Article 8.b. - Additional safeguards for the data subject -)

[Individual Participation Principle- An individual should have the right:]to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him (OECD; Individual Participation Principle – Subsection a.)

[Individual Participation Principle - An individual should have the right:]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 (OECD; Individual Participation Principle – Subsection b.);

Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information; (EU; Section 41)

Part II – Data Processing

8. Access to Data / Right to Amend (continued)

b. Amendment only

There must be a way for an individual to correct or amend a record of identifiable information about himself. (HEW 1)

Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information. (COP 1; Section 9)

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. (The Individual Participation Principle) (PPSC; Section 3)

*[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; Article 8.c. - Additional safeguards for the data subject)

*[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. (COE; Article 8.d. - Additional safeguards for the data subject)

Individual Participation Principle- An individual should have the right:]to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended. (OECD; Subsection d)

Part II – Data Processing

8. Access to Data / Right to Amend (continued)

c. Access and amendment

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. (DHS 1)

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. (Canada MC; Section 9)

Access - Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information. (FTC)

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. (Draft NSTIC)

Part III – Data Distribution

Please see Part II, section 6.b. for FIPPs that deal with data distribution limitations.

Please also see OIX Verb Taxonomy Tool for discussion of Data Distribution sub-categories.

Part IV - Other

9. Public Interest Exceptions

Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; protecting the data subject or the rights and freedoms of others. (COE; Article 9.2)

Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects. (COE; Article 9.3)

Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence; (EU; Section 43)

Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled; on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary; (EU; Section 45)

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 WP)

Part IV – Other

10. Other

The following FIPP provisions did not fall easily into any one of the foregoing categories.

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 1; Section 4)

Care should be taken in coding value judgments. (COP 1; Section 10)

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; Article 6)

No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article. (COE; Article 9,1)

In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned. (COE; Article 15,3)

[Individual Participation Principle- An individual should have the right:]to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial. (OECD; Individual Participation Principle – Subsection c)

Non Compulsory – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service. (ICAM; Section 3.3, 2.e.)

Non-discrimination. Participants in the OITF must avoid discrimination. Participants must not engage in exclusive dealing arrangements relating to the trust framework. (OIFT WP)

Interoperability. Software and hardware specified in the technical requirements of an OITF must conform to defined standards that promote interoperability. (OIFT WP)

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). (OIFT WP)

Redress. OITF Providers must ensure that all agreements under the OITF afford the parties an effective right and mechanism to seek redress. (OIFT WP)

Identity Provider *Bona Fides* - The TFPAP requires that Trust Framework Providers sufficiently review member Identity Provider *bona fides* to ensure that the member Identity

Provider has organizational maturity, legitimacy, stability, and reputation. (TFPAP Trust Criteria Assessment 3.3 (3))

V. OIX FIPPs Comparison Tool User Guide

What is this?

This is a tool to help develop legal and policy “Rules” for online and telecommunications data/identity systems.

How does it work?

The FIPPs Comparison Tool takes existing “fair information practice principles” from multiple jurisdictions and re-sorts their respective principles by logical categories of legal duties they impose on data collectors to perform or refrain from performing certain “data actions.” See OIX “Verb Taxonomy” for discussion of “data actions.”

Appendix 1 lists the 16 sources including sovereign jurisdictions, regulatory authorities, multinational organizations, and other governmental and private sources of FIPPs principles referenced in the FIPPs Comparison Tool tables. Each of these FIPPs sources reflects developed laws (and/or policies to guide laws) relating to Fair Information Practice Principles (FIPPs). Appendix 1 provides links to the original versions of those authorities.

This document (when finalized) will present the provisions of all of the FIPPs listed in Appendix 1, re-sorted by theme, with provisions reflecting each “theme” presented in a separate table. In this draft, a subset of the listed FIPPs is included in the tables.

For example, all of the provisions from the 16 different FIPPs relating to the theme of “data collection notice requirements” are presented together on one table, while all of the provisions relating to the theme of “user access to data to make corrections” are compiled on another table.

There are 10 separate tables (and a couple of sub-tables) in all (as reflected in the table of contents below), each representing a separate “theme” among the original FIPPs.

How can this help?

The purpose of the tool is to aid in the identification of themes underlying existing “traditional” FIPPs, to help inform, but not to limit, the consideration and creation of new and modified FIPPs to address current and future stakeholder needs.

Re-sorting by category of data system “actions” and practice enables the easy comparison of different FIPPs requirements, so that similarities and differences among different sets of FIPPs can be readily identified.

Similarities among FIPPs (particularly those from different legal jurisdictions) provide potential paths to the establishment of standard, “interoperable” legal specifications to support various notions of “privacy” worldwide.

This is a draft

These tables are a work in process. They do not yet include the relevant provisions of the U.S. Privacy Act of 1974, French law, German law, and the coverage of the European Union authority is incomplete. Distillation of the FIPPs from those and other sources is continuing.

In any event, these tables are not intended to present comprehensive coverage of all of the authorities in each listed jurisdiction. They are intended to provide “food for thought” in the consideration of natural candidates for legal standardization to help build online identity systems. Apologies are made in advance for any incompleteness reflected in the tables.

OIX is in the process of continuing and refining this analysis. The categories listed below are meant simply as a general guide to how the FIPP provisions might be grouped. It is expected that further discussion and analysis will refine and improve the analysis.

Like all OIX programs, the further development and maximum benefit of this material depends on content contributions from the broad identity community. Persons familiar with the laws of the represented jurisdictions and similar rules from other jurisdictions are encouraged to submit comments and suggestions to the OIX Advisory Committee. The initial treatment in this draft is intended for general reference and comparison. Users are strongly encouraged to consult with primary materials for definitive information regarding the FIPPs.

Other FIPP Tool review notes

The source of each listed set of FIPPs is referenced in parentheses at the end of each entry in the tables. The source lists the abbreviation for each FIPPs set (such as “HEW 1”), as well as a section number indicating where that particular provision can be found in each such FIPPs set. The cites, links to the FIPPs, and the abbreviation key are located at Appendix 1.

The term “data handler” as used herein is not a term of art, but is meant to generally reference a party that performs an action with respect to data, for which a duty is imposed under a FIPP provision. The responsibility for “data handling” is currently generally conceived of as being associated chiefly with commercial and institutional service providers (such as those of a so-called “Identity Provider” in an online identity “assurance” transaction) and government data collectors, but is recognized as potentially being broadened as non-commercial participants in social networks increasingly engage in similar data handling activities for both commercial and other purposes.

For a nicely summarized history and relationship among many of the FIPPs authorities referenced here, please see the excellent article by Bob Gellman, called “FAIR INFORMATION PRACTICES: A Basic History” at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf> . Mr. Gellman has no affiliation with OIX.

Please provide any comments to these materials to OIX at: [insert address here]

Appendix 1

List of FIPPs

HEW 1

U.S. Department of Health Education and Welfare

“Records, Computers and the Rights of Citizens” issued by the Secretary's Advisory Committee on Automated Personal Data Systems; Elliot Richardson, Secretary of the Department of Health, Education and Welfare (1973)

COP 1

Great Britain Committee on Privacy

“Report of the Committee on Privacy” chaired by Rt. Hon. Kenneth Younger, Chairman) (1972).

See Appendix B of the 1973 HEW Report for summary of report.

<http://aspe.os.dhhs.gov/datacncl/1973privacy/appenb.htm>

PPSC

U.S. Privacy Protection Study Commission

“Protecting Privacy in an Information Society” (ch. 13).

<http://aspe.hhs.gov/datacncl/1977privacy/toc.htm>

COE

Council of Europe

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1980)

http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt

OECD

Organization for Economic Cooperation and Development

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Privacy Act

U.S. Privacy Act of 1974

[5 U.S.C. §552a **To come**]

DHS 1

U.S. Department of Homeland Security,

Privacy Policy Guidance Memorandum (2008) (Memo. 2008-1)

http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

EU

European Union Data Directive

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

Canada

Canadian Standards Association Model Code

<http://www.csa.ca/cm?c=Page&childpagename=CSA%2FLayout&cid=1239124810319&packedargs=itemcontext%3Dca%252Fen%252Fnull&pagename=CSA%2FRenderPage>

Codified at:

<http://laws.justice.gc.ca/eng/P-8.6/20090818/page-1.html>

France

Original: Law on Informatics and Liberty 1/6/1978

Law of 1978, incorporating 2004 and 2009 amendments:

<< File: France-Privacy.pdf >>

Decree No. 2005-1309 enacted for the application of 78-17, incorporating amending decree of 2007:

<< File: France-Privacy-Decree.pdf >>

International Privacy Guide:

<< File: Westlaw_Document_13_07_54.doc >>

Germany

Federal Data Protection Law 1977, amended in 1990, 1994, 1997, 2002.

Currently unable to locate the 1977 and 1990 text in English for inclusion in tables.

Link to 1994 version at: <http://www.iuscomp.org/gla/statutes/BDSG.htm>

Current Version: Federal Data Protection Act



Federal Data
Protection Act.pdf...

Source: http://www.bfdi.bund.de/EN/DataProtectionActs/DataProtectionActs_node.html

Sweden –

Data Act of 1973: Text not yet located.

Text as amended in 1989 at: <http://archive.bild.net/dataprSw.htm>

Current Version: Personal Data Act 10/24/1998 replaced Data Act of 1973 (needed to be in compliance with [EU Privacy directive](#))



Personal Data
Act.pdf (66 KB)

Source: <http://www.datainspektionen.se/in-english/legislation/The-Personal-Data-Act/>

FTC

U.S. Federal Trade Commission

<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>

ICAM

U.S. Identity Credential and Access Management

Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3, Version 1.0.1, Release Candidate September 4, 2009

<http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf>

Draft NSTIC

U.S. National Strategy for Trusted Identities in Cyberspace (Public Draft)(2010)

<http://www.nstic.ideascale.com>

OITF WP

Open Identity Trust Framework White Paper

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

Appendix 2.

Proposed Notes for the Risk Wiki relating to the Fair Information Practice Principles (FIPPs) Comparison Tool

REVIEW NOTE: This Appendix 2 sets forth an extended discussion of how the FIPPs tool can help parties engaged in current trust framework development and drafting and in future legal standardization efforts, and its relationship to other trust framework development tools and processes. This discussion is intended to be considered for inclusion on the OIX Risk Wiki when it is made available online.

It is not necessary to review these notes in order to use the FIPPs Comparison Tool.

Standard “data action” practices can address “privacy” problems, not symptoms

Problem 1 – Complexity. Online “privacy” is multi-faceted. Discussions of current and future personal data and identity systems in different meetings and venues over the past several years have suggested that the concept of “Privacy,” as it is variously conceived and described worldwide, will continue to offer challenges to policymakers and system designers as they seek to address myriad issues of context, culture, and personal preference.

This tool and the OIX Verb Taxonomy Tool offer a proposed path to help deal with the complex, multi-faceted nature of modern “privacy.” The FIPPs Tool deals with existing authority, much of which was developed in a period prior to the time that the issues have taken on additional layers of subtlety and complexity. Nonetheless, this Tool demonstrates that somewhat standard FIPPs “categories” already exist among the various published FIPPs iterations; and it re-organizes the existing FIPPs provisions within those categories in anticipation of their further development as called for in the Department of Commerce Green Paper.

For a preliminary discussion of some of the more recent categories of potential “harms” associated with data, please see the discussion in the Verb Taxonomy Tool and relevant sections of the OIX Risk Wiki.

Problem 2 – Pace of change. As technologies (most importantly networked information technologies) are evolving, existing notions and concepts of “privacy” are revealing themselves to be insufficient (in granularity, subtlety and scope) as analytical structures for citizens and institutions to engage in full discussion of the contextually-appropriate balance points between the benefits of system integration to the individual, and perceived undue or otherwise “inappropriate” levels of “integration/intrusion” (aka “Privacy issues”). Standard “data action” rules created with processes that anticipate change can help to set stakeholder expectations and “normalize” online social communities, commercial markets, and political governance structures.

Problem 3 – Lack of guidance. Existing legal authorities in various jurisdictions only deal with a very narrow slice of the popular notions of “Privacy.” In the United States, for example, the law’s typical application of the “reasonable expectation of privacy” test in a particular fact

setting coaxes the analysis toward a broader, objective/community standard, but doesn't answer the question of what is "reasonable" in a given context (particularly newly-emerging digitally mediated contexts). Separate "data security" laws are more relevant to addressing "Level of Protection" (LOP) (for "leaky data pipes"), which doesn't cover all relevant LOC ("Level of Control") variables. [Link to LOC/LOP discussion here]

Effective future information and identity systems will need to be able to accommodate and support various perspectives on "privacy" robustly, flexibly, and at global scale (i.e., for multiple jurisdictions, cultures, and commercial, social and political settings).

This FIPP Comparison Tool is intended to help policy makers, attorneys and system developers to identify relevant current practices that can provide initial traction in setting up systems that can provide data subjects with the types and levels of "control" they need to achieve their "reasonable" expectations of privacy as that concept continues to develop.

Initial focus on privacy "practices," not privacy endpoints

This tool does not seek to establish a fixed "baseline" notion of "adequate privacy" for application in multiple settings. Instead, it seeks to identify commonly recognized practices and processes associated with the system operations and administration that are relevant in providing users with adequate "controls" that can give rise to satisfactory levels of user "privacy" experience whatever their level of "expectation" in a given context.

It is proposed that a set of operations and administrative practices, i.e., "Generally Accepted Privacy Practices" (GAPP), can help to form the process-oriented building blocks of a internet scale system that can help to address "privacy" in its various iterations, by permitting system designers, policymakers and ultimately users to select and apply those standard GAPP practices that are relevant to their privacy needs in a given context.

It is the proper performance of an identified set of such practices, in a given context, that can provide a data subject with an appropriate level of "privacy." In a sense, privacy will "emerge" from these and similar practices, much as it is currently perceived to result from a given set of appropriate offline practices. Thus, data subject privacy is "enabled" by system rules, rather than being "preserved" by them as a fixed point.

The focus is on the "practices" that can clarify and support simple, identified, balanced, cost-efficient, commercially viable, privacy and security-enhancing user-based controls. Thus, the system does not "serve up" privacy, but instead provides the functionality of assembled practices through which the exercise of the controls by the data subject can derive the desired "privacy" suitable for the context and user setting involved.

What subset of stakeholder needs do FIPPs currently address?

In general, FIPPs are directed primarily at individual data subject "needs," since they were generated originally to address concerns over intrusions upon individual rights in the face of

increasing data collection by governments, and developed subsequently to address similar concerns as data collection by commercial entities increased.

While all stakeholders in a particular trust framework benefit indirectly from the system regularity and predictability engendered by standard practices, current versions of FIPPs are directed primarily at establishing individual data subject rights. Specifically, each iteration of FIPPs addresses those rights that were thought to engender forms of individual data subject “control” at the time (and in the context) that they were each developed, so that data subjects could act to prevent various forms of “intrusion” in those contexts. FIPPs provides system “levers” to data subjects.

FIPPs and “Privacy”

The types of intrusions that were meant to be addressed by traditional FIPPs are of the same general type as those that are generally referred to as “privacy” issues in the current popular discussion. Notably, however, some of the “rights” provided in earlier FIPPs versions to enable control against “intrusions” have been strained by more recent data collection realities. It is for this reason that existing sets of FIPPs provide only a starting point for the present discussion.

For example, the “notice and consent” model that is captured in most FIPPs versions worked best when data collection events were infrequent, isolated and significant (such as in the 1970s, 1980s and 1990s when FIPPs were first developed and codified into various laws), but their effectiveness has been challenged by the new reality of ubiquitous data “micro-collection” in real time, as “data entry” is performed simply by using the system, and where literally trillions of system entries and calls for information occur daily.

In the new context, the provision of “traditional” notice, and the requirement of consent for each act of collection and for each use of data about an individual (particularly in the era of “behavioral advertising” and other sophisticated data mining and correlation practices), could quickly swamp the individual with a new form of spam, i.e., “notice-and-consent spam,” that could cause the identity system equivalent of an inadvertent “denial of service” attack from the perspective of the data subject. This is an example of how existing information practice principles will need to continue to evolve in order to be appropriately called “Fair.”

Which stakeholder needs are not addressed in FIPPs?

Since they were developed to address “privacy” needs, the earlier versions of FIPPs were not directed at addressing the needs of commercial data subjects (XYZ Inc.com), employee and agency issues (where an individual’s online identity is used in a representative, not personal, capacity), or the data system needs of relying parties, identity providers and other commercial and individual data handlers and system service providers (including assessors, auditors, online dispute resolution service providers and the like). That is not to say that those parties don’t benefit indirectly from the system “normalization” of FIPPs; they do. They are not, however, the primary intended beneficiaries of current FIPPs.

Traditional FIPPs were designed to address one main vector of system design, i.e., the needs of individual data subjects to be protected from intrusion by data collectors (government and/or commercial). It is a very important piece, but only one piece, of the guidance needed for a comprehensive set of legal rules to document and render enforceable all of the mutual promises of all federated data/identity system stakeholders to perform their respective duties in system-consistent ways.

FIPPs and current “privacy” concerns relate to “intrusion”

The recent FTC proposal entitled “Protecting Consumer Privacy in an Era of Rapid Change” [\[link\]](#) provides a helpful structure for referencing categories of harms. On page (iii) it notes that the “harm based model” of enforcement was directed at “protecting consumers from specific harms – physical security, economic injury, and unwanted intrusions into their daily lives.”

Harms to Person and property

Harms to property and person are different than “intrusion” harms. For instance, in the case of property and personal harms, online identity information is typically just the “instrumentality” of the crime (like the “getaway” car in a bank robbery). In other words, the identity information is procured (through “pretexting,” social engineering, or other “identity theft” activities) in order to carry into effect the true object of the overall plan, which is to use that data in order to perform other illegal or unauthorized activities that cause harm to property of person. These are typically some form of monetary theft or otherwise engaging in unauthorized access to stored information or information system functionality for purposes that are inconsistent with one or more of the authorized users of that system. Where traditional harm to person or property is involved, the unauthorized access to data may be intrusive, but the focus is on the more familiar and legally cognizable harm caused by such person or property.

An example can illustrate the distinctions drawn in the prior paragraph. If a person’s credit card number is “taken,” it is clearly an act of unauthorized access to data (a data security issue), but it is less clear what aspect, if any, of their “privacy” was compromised. It is hard to say that a person has an interest in a specific account number, other than with respect to it providing them with access to consumer credit arrangements for their convenience.

That is not to say that there is no harm when there is unauthorized access to a payment card account number; clearly there is. The integrity of the consumer credit system upon which they and other parties rely is compromised to the extent that unauthorized parties have access to account numbers. Trust in the system is supported by Reg. E which limits the consumer liability to \$50 in most circumstances. To foster trust in the system that is needed for adoption of the identity system supporting modern consumer credit, the “trust framework” of the PCI-DSS rules (supported by Reg. E as a form of “market-normalizing” background law) work collectively to shift responsibility for systemic risk away from the consumer (but do require the consumer, as data subject, to engage in certain system-friendly duties, such as protecting account numbers and passwords, and checking periodic statements, etc.).

Intrusion harms involving data – protecting the “Stochastic Self”

In contrast to traditional bodily and property harms, the harms that are categorized as “intrusion” are experienced by the data subject more directly, typically as a proximate result of the unauthorized access to data. Applying the concept of “intrusion” in the online context itself suggests that it is the unauthorized access itself that results in the harm, rather than the subsequent use of data as an instrumentality of a later crime.

“Intrusion” is an analytically slippery concept at the foundation of much traditional legal analysis where there is a tension at the boundary between individual rights and group interests. It is challenging enough to define intrusion where a physical feature provides a handy reference for placing the boundary between individual and the “intruding” group (such as the fourth amendment’s reference to the walls of the home, or the skin of the person). The challenges of defining “intrusion” are even greater in the online data context where the boundaries of individual “identity” to be protected against undue intrusion are only manifested as a contextually-selected subset of data that is spread out across the entire distributed information system we call the internet.

How do you put a digital “skin” around the thousands of computers that contain a person’s social security number? How do you define “intrusions,” and which should be the subject of the formal rules of laws, particularly where the other end of the intrusion “stick” is “integration,” and given the myriad benefits of new interactions that are simultaneously “intrusive” and “integrative.”

The greatest challenge may not be in understanding “how” to defend against intrusion online; that will be done with Technology Tools and Legal Rules (such as the rules set forth in FIPPs). Technology tools and Legal Rules are the “skin” of the digital “self.” It is likely, however, that seeking to understand “what” is to be protected will present greater challenges. Stated briefly, in the statistical analyses that support behavioral advertising and other data analyses and correlations, how do you measure intrusions on a digital “stochastic self,” and what is the nature of that “harm” and “intrusion.”

One potential approach is to distinguish raw “data” from observed “information.” Applying this distinction, data carries information, but “information” only arises when data is observed in a context.

One suggestion is to apply a “results oriented” analysis that leaves data relatively unregulated so that it can “flow” until such time that it is “assembled” by an “observer” in a manner that enables the identification of an individual. This action of “assembly;” a so-called “recognition event,” could be the objective trigger that has legal effect.

Since an “intrusion” is possible only when the data is correlated with a person to be potentially “harmed” by the intrusion, the establishment of a “recognition event” with legal effect serves to provide a basis for causing an “intrusion” concept to be legally cognizable. Consider an observer that collects various innocuous, publicly available data into a profile from which they can identify an individual. As soon as that “collection” activity results in the “aha” moment when a person is identified, that volitional act by the observer is the “recognition” event. At that point, it

may be appropriate to ask the observer to consider the implications of the Recognition Act for the data subject. For instance, the observer (the data collector, transferee or other user) could consider limitations (such as rules of “contextual appropriateness and distribution norms), regulations, measurement, compensation and other legal implications associated with the “discovery” of an individual person through a recognition event that takes place with respect to a set of data for purposes of limitation,

Defining the “rights” intruded upon

Thus, the greater challenge may be in deciding where that boundary (the “skin”) should be positioned so that the “intrusion” can be defined and thereby addressed, and in deciding what “controls” should reside with the individual for a given piece of data.

That is not an entirely objective question, and its resolution depends on a combination of influences from at least three separate contexts where individual/group relationships are defined; the community and social rules, the market and commercial rules and politics and governance structure rules. Effective FIPPs will provide baseline protections of the interests of individuals *vis a vis* the groups balanced with group interests in each of these contexts, particularly since they all rely on the same resources, i.e., the *common, networked communications grid* of the internet, and the *common, shared pool of data* that it creates, stores and serves to all users in a variety of contexts.

It will be ultimately be insufficient to seek to define the nature of future intrusions solely with reference to how prior intrusions were resolved. This is because the internet enables interactions and transactions that are not directly comparable to those possible before. A blog entry, social network post, or “tweet” enables a single individual to communicate information to thousands of people simultaneously; e mail enables instant and asynchronous communication with remote parties; internet search enables instant access to context-relevant information about another person to supplement traditional behavioral cues, etc. etc.

Interactions (i.e., the transfer of information between sender and receiver) such as these have no direct corollaries in prior information systems, with a corresponding lack of guidance as to where to draw the line between desired “integration” and undesirable “intrusion” that these new forms of interaction can cause. This is behavioral “white space.” Since behavioral customs typically precede and inform formal rules and laws, there is little developed “community or industry practice” on which to base formal rules to define “intrusion.”

The good news is that the lack of guidance also provides ample room for designing the web of mutual enforceable promises that balances all stakeholder needs. That exercise will require mechanisms through which the equivalent of stakeholder “discussions” can take place. The OIX risk wiki is designed to support that persistent, ongoing, multi-layer, multi-stakeholder, internet scale “conversation” associated with “pre-listed” trust frameworks while they are in development. The OIX listing Service is intended to support the continued “conversation” in the form of market feedback about published, certified trust frameworks.

“Intrusion” protection will be limited by the capacity of deployed Tools and Rules to protect

At any one point in development, the overall system's ability to offer reliable intrusion protection will be limited by the then-current capacity of its various "Tools and Rules" to offer such protection. Those Tools will develop and the Rules will gain efficacy as they are more broadly adopted (creating the valuable and desirable "network effects" that are variously called "markets," "communities," and "governance structures" in the commercial, social and political contexts respectively), but they will always "lag" behind needs. Thus, to some extent, the "boundary line" that positively defines online "identity integrity" and negatively defines "intrusion," will be defined indirectly, by the extent and reach of the FIPPs, how they are rendered enforceable through FIPPs-consistent contracts and laws, and how well the technology can be configured to handle data reliably, consistent with such rules.

Intrusion protection will need to be dynamic

At the risk of applying a metaphor of conflict instead of resolution, the concept of this moving identity "boundary" might be roughly analogized to the efforts of a line of soldiers defending a series of "positions" (each a "boundary") on a battlefield. They continue to defend against intrusion of their enemy, even as their position alters and moves. It is anticipated that the accelerating pace of change and the perceived "intrusions" that it will introduce will necessitate similar flexibility with strength in defining the dynamic "boundary" of the rights of the individual to exercise "control" regarding information (whether stored information ("data at rest") in the system, or transferred information being communicated ("data in motion") through the system) about them in a given context that is embedded in the larger information system.

In the case of online identity, rather than being resolved in a battle, the context-dependent boundaries will be most effectively resolved (and periodically revisited) through consensus among stakeholders, all of which benefit from more certain rules, and all of which face the common "enemy" of exponential increase in information, and the corresponding exponential increase in system complexity, disorder, risk and cost that it spawns.

FIPPs offer guidance for constructing trust frameworks

FIPPs offer guidance for constructing trust frameworks that are "interoperable" on "privacy." This opens up possibilities for greater data flow across trusted networks, since jurisdictions and their residents can do an "apple to apple" comparison across jurisdictions to more readily identify those jurisdictions that have embraced similar FIPPs to inform the construction of information systems that offer privacy protection consistent with that which they offer to their citizens and residents. Tools and Rules applicable to future online data/identity systems will be documented in Trust Frameworks. FIPPs inform the Tools and Rules that are directed at supporting the interests of individual data subjects, and indirectly support other stakeholder interests. Broad adoption of Trust Frameworks enables the network effects called "community" (social network effect), "markets" (commercial network effects) and "governance structures" (political network effects). The achievement of these network effects depends on broad adoption.

Trust Frameworks are successful if they are broadly adopted, enabling the “network effects” described above. Adoption can be accelerated (advancing desirable network effects) if a system is built to address all stakeholder needs. Trust Frameworks that are built based on processes that enable stakeholders to express and pursue their respective needs in a consensus-building process that balances needs and addresses potential conflicts, will likely enjoy rapid adoption by the participating stakeholders. FIPPs provide “focal points” for standardization of the legal rules that protect individual data subject interests in those processes. Through that mechanism, FIPPs can help to promote privacy standards and hasten the adoption of standardized systems.

In this way, FIPPs can be “baked in” to Trust Frameworks helping to form an “upwardly compatible legal stack.” That baseline of fair principles provides mutual benefit to all stakeholders associated with digital identity creation, integrity and control (which yields “privacy” protection), risk and liability reduction, system simplification, transparency and ease of use, and market expansion, innovation, valuation, monetization and other benefits.

How do FIPPs relate to LOA and other data/identity system metrics?

FIPPs principles are separate from, but closely related to, other sets of principles that inform the practices and duties that are associated with the “Levels of Assurance” (“LOA”) system metric first established by the U.S. Government, and proposed “Levels of Protection (“LOP”) system metrics. Each potential metric is intended to represent a “roll up” of the interests of a generalized “class” of participant in the online identity trust triangle. These system metrics also act as an indicator of system performance on several vectors. Finally, by offering “choice” to system stakeholders, they act as a sort of virtual “system lever” to enable system participants to dynamically “tune” information systems that they rely on in a specific context.

Specifically, the LOA metric provides *relying parties* with a “control lever” that can be applied to select the type of credential that they are offered by the system (at either LOA 1, 2, 3 or 4) to match their *assurance* needs. Mature LOC and LOP metrics could offer “control levers” to the data subject and the identity provider, respectively, to help achieve their respective system goals. To the extent that they offer relevant points of interaction with the larger system, the system metrics of LOA, LOP and LOC can act as starting points for the design, development and deployment of UIs for the different “user groups” to interact with data/identity systems. More information on these metrics can be found at [link to OIX website].

A proposed system metric for “Privacy” practices

The potential set of standard “legal specifications” roughly outlined by FIPPs is referred to in this material as “Generally Accepted Privacy Practices” (“GAPP”). A proposed identity system metric that GAPP could inform has been referred to as a “Level of Control” or “LOC,” in recognition of the relationship between providing users with the elements of control they need to achieve their respective expectations of privacy and security, balanced with their individual levels of desire to have access to the various benefits of network integration. It is expected that stakeholders, including data subjects, will desire that LOC can vary within bounds by context.

Standardizing toward a system metric

A standard set of GAPP Rules could be a toolkit from which different combinations of “privacy-preserving techniques” are selected for application in a specific setting to achieve the desired level of “privacy.”

When fully developed, and broadly adopted, a set of GAPP could be viewed as sufficiently reliable and predictable to warrant its quantification and presentation in an information system metric referred to as the “Level of Control” or LOC. Establishment of an LOC system metric would require the “scaling” or “weighting” of GAPP variables, and a risk analysis similar to that presented in NIST 800-63 (which unpacks the variables associated with the LOA 1-4 measure), but instead of evaluating risks to property and person as for LOA, taking into account the various perceived “risks” (each an “Intrusion” associated with privacy violations. The initial scale for LOC is proposed to be 1-4, to match the scale for the “Level of Assurance” measure developed by the U.S. Office of Management and Budget and the National Institute of Standards and Technology.

Notably, by applying the 1-4 scale to the three separate proposed metrics, i.e., LOA, LOP and LOC, it is possible to describe 64 different system states ($4 \times 4 \times 4 = 64$). Future maturation of the metrics could yield additional gradations which would yield an increased number of potential states that could be described.

Prior to such a quantification exercise, this FIPP Comparison Tool is intended to aid in the review of some of the baseline standardization opportunities for LOC as support for the “Privacy” related services of identity systems. To the extent that a subset of the listed FIPPs reflects current institutional practices (of governmental and commercial entities) in multiple legal jurisdictions, they offer potential “low hanging fruit” of system LOC interoperability. This translates into potential system cost savings, increased reliability and predictability for users, and expanded potential markets for personal data/identity services.

The proposed LOC system metric would group together, and ultimately quantify, those data system control practices that are directed toward enabling data subjects to achieve their respective “expectations of privacy.” Perhaps more importantly, the LOC metric provides a focal point for the collective development of the norms and “best practices” for privacy so that future expectations and information system performance better align.

How does LOC relate to LOP?

The proposed Levels of Protection (“LOP”) metric (in contrast to LOC) is also generally relevant to privacy, but more to the extent that it captures those practices associated with preventing *third party* unauthorized access (preventing “leaky data pipes,” aka data theft). The prevention of unauthorized third party access to data is arguably a subset of potential information “distribution” harms, and the inclusion of “security” requirements as part of FIPPs speaks to this relationship. However, prevention of the harms associated with third party unauthorized access to data has attracted an independent, developed body of law that plays a distinct role in preventing identity theft and issues of overall system integrity, and importantly in normalizing data handler risk and liability, such that it warrants a separate LOP metric. LOC, by contrast,

involves a potentially broader set of issues and practices that are of interest to data subjects, including individuals acting in their capacity as citizens, consumers, and members of society.

The various versions of FIPPS are more similar than different

A brief review of the draft tables reveals that the vast majority of the provisions of different FIPPs address some subset of the same 9 FIPPs themes (with a few less common provisions listed in section 10).

This broad similarity encourages the comparison of provisions of different FIPPs from different jurisdictions to identify the areas of potential legal standardization that can provide potentially helpful starting points for the construction of future legislation and private agreements (contracts, TOUs, etc.) to structure global identity systems.

It also suggests those areas that could already be sufficiently “normalized” that relatively little effort might be required to achieve additional standardization into a “legal specification” that then could help to form the basis for future commercial and open source identity solutions, products and services. Future work in this area can develop these and other potential system and cost benefits.

It is important to note that this analysis is just a starting point. Some of the FIPPs listed are over 30 years old, and may not be sufficiently up-to-date to yield full insight into current “best practices.” It is important that the FIPPs be evaluated for what they are, sets of suggested practices that resulted from different investigative and/or legislative initiatives in different jurisdictions as the global information system has developed. Some were directed toward governmental practices, others toward commercial practices, but many apply to both.

Despite their vintage, several FIPPs sets do reflect current binding background authority and legislative and administrative guidance in jurisdictions with significant populations of online and telecommunications users. As such, they provide a form of *de facto* standardization in those jurisdictions, and therefore are at least a “starting point” for developing more modern, broader, interoperable practices. It is anticipated that as system users (including data subjects, relying parties and identity providers) become more familiar with the LOC concept, new and modified practices will emerge as additional candidates for adoption as consensus-based practices.

The OIX Verb Taxonomy deals with a more extended set of data-related practices (including various sub-practices) that reflects a more recent examination of potential data-harms than that underlying traditional FIPPs. Parties working on expanded versions of FIPPs are invited to review and contribute to the development of both the OIX FIPPs Comparison Tool and the OIX Verb Taxonomy Tool, in addition to the online OIX Risk Wiki of which these tools are a part.

We have enabled networked information systems to provide users with “privacy” before

The history of information communications (such as postal mail, telegraph and telephone communications), each is a story of insecure networks that became “private” (through controls using “Tools and Rules”) because people wanted them to be private. Privacy is not just about

what people expect, but about what they desire. Privacy is something we construct through norms and the law because we desire it. Thus, we call upon the law to protect privacy because we experience a lack of privacy and desire to rectify that situation, not because we already expect it.¹ The law reflects our needs and shapes future expectations. Development of FIPPs can help to do both.

¹ “The Meaning of Privacy – Appeal for a Pluralistic Definition of the Concept of Privacy,” Daniel J. Solove, in *Open* 2010/ No. 19 “Beyond Privacy”