LEVELS OF PROTECTION (LOPS)

Mary Rundle and Sue Glueck[1]

Proposal Submitted to the ISO Privacy Standards Conference
(October 8 and 9, 2010 – Berlin, Germany)

Introduction

A common source of distrust in online interactions today stems from people's lack of confidence that their identity information[2] will be treated with care. This white paper proposes the development of levels of protection (LOPs) to enable a person disclosing identity information (a Discloser) to have assurance in advance that it will be treated with appropriate protection by the party to whom it is disclosed (the Receiver).[3]

The term "levels of protection" as used here refers to degrees of data protection applied to identity information, with progressive levels allowing parties who disclose or receive identity information to know in advance how it is to be treated. Symbols or icons associated with progressive levels (e.g., LOP1, LOP2, LOP3, LOP4) may indicate (a) the public policy commitments that go with a given level, (b) corresponding explanations of the public policy commitments, and (c) metadata that is machine-readable. Public policy commitments of the LOPs proposed here are drawn from pre-existing arrangements or "regimes" for data protection, to reflect different regulatory orientations. Language for the data protection principles was drawn from concepts contained in a variety of sources, such as the *Privacy Framework* of the Asia Pacific Economic Cooperation (APEC) group, the *Privacy Guidelines* of the Organisation for Economic Cooperation and Development (OECD), the *Fair Information Practice Principles* developed by the U.S. Federal Trade Commission (FTC), and the *Data Protection Directive* of the European Union (Directive 95/46/EC). Combinations of data protection principles at the different levels will serve as public policy criteria against which parties dealing with identity information can be assessed and certified in terms of their practices, for example as part of the assessments and certifications based on an ISO/IEC standard such as the ISO/IEC 27000 series.

By signaling the strength of protection offered by Receivers of data, LOPs can thus help Receivers to indicate the level of protection they offer and enable Disclosers to opt for protection levels according to context. In this way, LOPs can facilitate exchanges that conform to law and give contracting parties greater predictability and the ability to negotiate.[4] In time, jurisdictions hopefully will be able to formally establish that a particular LOP meets their legal requirements.

---

[1] Ideas in this paper have developed through conversations with Beverly Allen, Ronny Bjones, John Bradley, Stefan Brands, James Brown, Malcolm Crompton, Trevor Freeman, Jeffrey Friedberg, Dan Hitchcock, Rainer Hoerbe, John Howie, Rushmi Malaviarachchi, Eve Maler, Anthony Nadalin, Mike Ozburn, Christian Paquin, Kai Rannenberg, Drummond Reed, Don Schmidt, Philip Stradling, Hannes Tschofenig, Don Thibeau, David Turner, and Craig Wittenberg, as well as a number of government officials concerned with data protection.

[2] The term "identity information" is used here rather than "personal data" or "personally identifiable information (PII)" because the person or entity in question might not be identifiable; he, she, or it could be anonymous or pseudonymous. "Identity information" includes both authentication information for establishing that a person or an entity is who he, she, or it claims to be (which may or may not include an identifier), as well as attribute information for sharing details about that person or entity. Such identity information is sometimes referred to as "claims".

[3] By way of caveat, it must be stressed that this proposal for LOPs is put forward as a building block, but not the entire solution, for empowering users and facilitating the expression of data protection requirements and capabilities.

[4] Note that there could be a dynamic nature to this arrangement as multiple LOPs could be in play on both sides to accommodate different contexts. In other words, there might be multiple choices of what a Discloser wants versus what a Receiver is willing to offer – hence, the negotiation.

Background

Because a given party may sometimes receive identity information and at other times disclose identity information, this paper uses the terms "Receiver" and "Discloser" to connote the role being played and the expectations that go with that role. By way of example, a bank could serve in both capacities: As the bank receives identity information from a person establishing a bank account, the bank is in the role of "Receiver", while the person is the "Discloser". The person may later ask the bank to provide some of his bank details to another party such as an e-commerce site, in which case the bank becomes the Discloser and the e-commerce site is the Receiver. In both cases, the Discloser wants to know that the Receiver will treat the information with appropriate protection, while the Receiver wants to know that the information sent by the Discloser is reliable.

With regard to this latter aspect – i.e. the Receiver's desire to know that the information sent by the Discloser is reliable – it should be noted that the U.S. National Institute of Standards and Technology (NIST) has developed a four-level standard to signal "Levels of Assurance" (LOAs) for authentication. LOAs concern both identity proofing processes (how a person proved who he or she was when registering for a new digital identity), plus the strength of the actual authentication methods used when that person subsequently logs in to perform an identity-based transaction.[5] A fitting complement to LOAs would be LOPs to represent the Discloser's interests in data protection with a four-level standard.[6]

Public policy might take a "laissez faire" approach and allow the Discloser to choose the LOP, or it may be that the law prescribes LOPs for various contexts, for example to ensure adequate protection for sensitive information. If a bank were in the role of Discloser, such an institution would likely grow familiar with the fine-grained details of requirements. However, an individual in the role of Discloser might not want to expend the effort or might not be able to grasp the implications of choices in different contexts; to avoid dealing with details, people might choose to follow the recommendations of trusted associations or trust marks.[7] For instance, members of the American Association of Retired Persons (AARP) might wish to follow its recommendations by default; AARP might recommend LOP2 for posting a comment to a blog and LOP4 for transferring health information, and technologies could kick in to apply the appropriate choice according to the context.

Designed to Work with the Open Identity Trust Framework (OITF) Model

Another way to spare individuals from having to discern which LOPs make sense in which contexts would be to leave it to a given "trust framework" to include LOPs as they establish technical, operational, and legal requirements for exchanges involving identity information.

[5] The international community is considering adopting standards similar to the NIST standards in work of the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO).

[6] Four levels are proposed because (i) the LOA standard for the Receiver's interest has four, and using four for LOP would therefore help connote the complementarity, and (ii) four levels offer a range of choices without offering so many as to be confusing for the parties involved.

[7] To the extent that trust marks are viewed as an answer to the difficulty of users' understanding the meaning of choices in specific contexts or as addressing the need for convenience, there is still the problem that users must understand what trust marks provide in terms of guarantees.

According to the Open Identity Trust Framework (OITF) model[8], if policymakers wish to set parameters for exchanges involving identity information, they may mandate that the exchanges take place within the bounds of a trust framework that meets their technological, operational, and/or legal requirements. A "trust framework provider" (TFP) is the entity that then implements those requirements in a trust framework. The TFP does so by having assessors apply objective criteria to certify that "identity service providers" and "relying parties"[9] can meet policymaker requirements. The TFP then runs a certification listing service to show which parties have been certified. In any given OITF, these parties are legally bound by a set of agreements; those agreements are to follow the "Principles of Openness"[10] that are included with the model for the sake of accountability, transparency, and open competition. Because the OITF model is designed for implementing public policy requirements such as data protection, LOPs would be a natural fit. Specifically, LOPs would enable trust framework participants to understand each other's conditions and capabilities, and they would equip policymakers better to understand which trust frameworks could comply with their jurisdictions' data protection laws.

Applicable to Cloud Computing

The LOP approach is also applicable to cloud computing. As a service provider receives identity information and in turn stores it in an outsourced cloud database, that party switches from playing the role of a Receiver to playing that of a Discloser; LOPs' flexibility allows that service provider to verify that its cloud provider can perform at that same level. Simply put, on a micro level the service provider is able to provide services at lower cost and indicate its data protection practices in a way that allows the end user to efficiently compare against his or her own requirements (whether legal or otherwise). The end user obtains cheaper services with appropriate data protection; on a macro level, governments can say if a given level offers comparable protection to what their jurisdictions require, thus facilitating compliance and enabling the legal provision and consumption of services regardless of the location of data.

Public Policy Requirements Based on Pre-Existing Arrangements

To advance the Discloser's interests in data protection, this white paper recommends the development of LOPs that all address the same data protection principles but that do so to progressive degrees: the higher the LOP, the stronger the afforded protection. The data protection principles addressed are collection limitation, notice, choice, use, data quality, security safeguards, right of access, accountability, onward transfer, and permitted exemptions.[11] Each of these

[8] See the white paper entitled, "The Open Identity Trust Framework (OITF) Model" by Mary Rundle (managing editor and co-author), Eve Maler, Anthony Nadalin, Drummond Reed, and Don Thibeau (available for free download at: http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/oitf.aspx).

[9] In recent years, some exchanges involving identity information have been described as having three primary parties: a user; a "service provider" or "relying party" with which the user wishes to interact; and an "identity service provider" or "identity provider" that releases identity information to the relying party at the behest of the user. (To translate into terms used in this paper, the service provider/relying party is the Receiver, and the identity service provider is the Discloser acting on behalf of the user/individual.) The user could be a natural or legal person, or a device under a person's control. If the person who is the user is not the data subject, the data subject's rights must still be honored.

[10] The Principles of Openness have the following labels: Lawfulness, Open Reporting and Publication, Ombudsmen, Anti-Circumvention and Open Disclosure, Non-Discrimination, Interoperability, Open Versioning, Participant Involvement, Data Protection, Accountability, Auditability, and Redress. (For details, see the white paper referenced in footnote 8.)

[11] These categories are drawn from international approaches to data protection that have gained traction over the past few decades, as explained in the next paragraph.

principles at LOP1 will be met with relatively light data protection, whereas each of them at LOP4 will be met with rather strict protection.

Annexes A and B propose public policy requirements to cover data protection principles at each LOP, with technologies and operational methods to be suggested for each principle at each level. The specific LOPs proposed in the Annexes draw from pre-existing legal arrangements or "regimes" for data protection, to reflect different regulatory orientations, including the *Privacy Framework* of the Asia Pacific Economic Cooperation (APEC) group, the *Privacy Guidelines* of the Organisation for Economic Cooperation and Development (OECD), and the *Data Protection Directive* of the European Union (Directive 95/46/EC).

Going Forward

Developing this LOP concept will require a multi-disciplinary effort. For the public policy piece, a group with international data protection expertise needs to check proposed principles at the LOP levels with a view to refining requirements. For the certification criteria, experts in the ISO/IEC 27000 series need to say what would give effect to each public policy principle at each of the four levels. Institutionally, in addition to assessment and certification processes like the ISO/IEC 27000 series, there may need to be providers of a listing service, auditors, and possibly a governance mechanism.

Please send comments on this white paper to LOPfeed [at] microsoft.com, with the subject line reading "comments on LOP paper".

ANNEXES: Tables Showing Data Protection Principles and Levels of Protection (LOPs)

These Annexes to the paper entitled "Levels of Protection" present four ascending levels of protection (LOPs). Each arrangement covers the same core principles, and together they represent a continuum in approaches ranging from lighter to heavier data protection requirements. The public policy provisions suggested here were drawn from concepts contained in a variety of sources, including the Asia Pacific Economic Cooperation (APEC) *Privacy Framework*, the OECD *Guidelines on the Protection of Privacy*, the *Fair Information Practice Principles* developed by the U.S. Federal Trade Commission (FTC), and the EU *Data Protection Directive* (Directive 95/46/EC).

Annex A contains tables arranged according to the core data protection principles. Each table suggests public policy approaches to achieve LOPs for the particular principle. To indicate how protection increases with each successive level, additions in public policy obligations that accrue from one level to the next are marked in red. Annex B takes the same material and compiles results according to the four LOPs, showing how they address data protection principles. Each table here suggests the collection of public policy that might be used to address all the data protection principles at a degree of rigor appropriate for that LOP.

Technological and operational[12] approaches corresponding to the public policy approaches may be developed by experts such as ISO/IEC 27000 series assessors and certifiers.

ANNEX A

ANNEX B

[12] Technological approaches might include, for example, product version levels, system configuration, settings, and protocols. Operational approaches might address, for example, asset management, access control, and disaster management.

A. COLLECTION LIMITATION

	Public Policy (red font indicates intensification from previous level)
LOP1	Receiver may collect identity information if it is relevant to stated purposes (which may be very broad). Publicly available identity information is not subject to these limits. Receiver should obtain the identity information by lawful and fair means.
LOP2	Receiver should limit the collection of identity information. Publicly available identity information is not subject to these limits. Receiver should obtain the identity information by lawful and fair means.
LOP3	Receiver must limit the collection of identity information to what is proportionate for the specific purposes for which identity information is used. Receiver must obtain the identity information by lawful and fair means. Identity information must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information was collected or for which it is further processed.
LOP4	Receiver must limit the collection of identity information to the minimum necessary for the specific purposes for which it is to be used, and Receiver must follow best practices for preventing correlation/the linking of transactions and re-identification. Receiver must obtain the identity information by lawful and fair means. Identity information must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the information was collected or for which it is further processed.

B. NOTICE (FACT OF COLLECTION, PURPOSE SPECIFICATION, CONTACT POINT, ETC.)

	Public Policy (red font indicates intensification from previous level)
LOP1	If the identity information is not already publicly available, Receivers should give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; and what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information. In terms of timing, Receivers should take all reasonably practicable steps to ensure notice is before or at time of collection, but if not then, as soon after as practicable.
LOP2	If the identity information is not already publicly available, Receivers should give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information; general practices and policies; and subsequent changes of purpose. In terms of timing, Receivers should give notice not later than at the time of data collection.
LOP3	Unless the identity information is subject to a Permitted Exemption regarding notice, Receivers must give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information; general practices and policies; subsequent changes of purpose; and whether the submission of information requested is obligatory or voluntary and possible consequences of failure to submit it. In terms of timing, Receivers must give notice not later than at the time of data collection. Notice requirements apply even when the relevant individual is not the Discloser, although some flexibility is allowed in terms of timing and in case offering notice would be overly burdensome.
LOP4	Unless the identity information is subject to a Permitted Exemption regarding notice, Receivers must give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information; general practices and policies; subsequent changes of purpose; whether the submission of information requested is obligatory or voluntary and possible consequences of failure to submit it; and the security safeguards. In terms of timing, Receivers must give notice not later than at the time of collection. Notice requirements apply even when the relevant individual is not the Discloser, unless such notice would be impossible because of applied protection measures (de-identification measures). If identity information is disclosed under a trust framework, the trust framework provider (TFP) must ensure that there is a publicly accessible registry of participants and their practices with respect to the specific interactions that take place under that trust framework. (See the white paper on "The Open Identity Trust Framework (OITF) Model", noted in the main body of this "Levels of Protection" paper.)

C. CHOICE

	Public Policy (red font indicates intensification from previous level)
LOP1	Individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to *opt out* of the arrangement.
LOP2	Individuals must be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to *opt out* of the arrangement.
LOP3	Individuals must be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to *opt in* to the arrangement. Individuals have a right to object to the use of their identity information. This right may be exercised at any time and, if justified, the Receiver may no longer use the identity information concerned. Such requests will in any case be justified if the relevant individual opposes the use of his identity information for marketing purposes. Except in cases covered by applicable Permitted Exemptions, individuals have the right to oppose decisions being made about them which would significantly affect them based solely on automated processing of their identity information.
LOP4	Individuals must be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to *opt in* to the arrangement. Individuals have a right to object to the use of their identity information. This right may be exercised at any time and, if justified, the Receiver may no longer use the identity information concerned. Such requests will in any case be justified if the relevant individual opposes the use of his identity information for marketing purposes. Except in cases covered by applicable Permitted Exemptions, individuals have the right to oppose decisions being made about them which would significantly affect them based solely on automated processing of their identity information. Where applicable law requires and the state of the art enables such implementation, the Receiver shall enable individuals to take data that they have contributed in one context and bring ("port") it to different contexts as the individual desires. Where applicable law requires and the state of the art enables such implementation, the Receiver shall follow best practices to allow individuals easily to set default preferences for the treatment of their identity information.

D. USE (LEGITIMATE; PROHIBITED)

	Public Policy (red font indicates intensification from previous level)
LOP1	Receiver should use identity information only (a) to fulfill the purposes of collection and other compatible or related purposes for which notice was provided; (b) when necessary to provide a service or product requested by the individual; or (c) as permitted by applicable law.
LOP2	Receiver should use identity information only (a) to fulfill the purposes of collection and other compatible or related purposes for which notice was provided; (b) when necessary to provide a service or product requested by the individual; or (c) as permitted by applicable law.
LOP3	Except in cases covered by Permitted Exemptions, Receiver may use identity information only: with the consent of the individual; to provide a service or product requested by the individual; when necessary for the performance of a task carried out in the public interest or by authority of law; or when necessary for the purposes of the legitimate interests pursued by the Discloser or a Receiver provided the privacy interests of the individual are not disproportionably affected. Trust Framework Providers shall only permit Receivers to use sensitive identity information with the opt-in consent of the individual, except that sensitive identity information may be used without consent: - if the use is necessary in an employment relationship where adequate safeguards are in place; or - to protect vital interests where the individual is incapable of consenting; or - where the Receiver is a non-profit organization that the individual is in contact with provided that the sensitive identity information is not disclosed to third parties without the consent of the individual; - if the individual has made the sensitive identity information public; or - if necessary in connection with legal claims; or - if related to the provision of medical care or the management of health-care services by health professionals; or - when necessary for the performance of a task carried out in the public interest or by authority of law; or - when necessary for the purposes of the legitimate interests pursued by the Discloser or a Receiver provided the privacy interests of the individual are not disproportionably affected.
LOP4	Except in cases covered by specific Permitted Exemptions, Receiver may use identity information only: with the explicit consent of the individual; when necessary to protect the vital interests of the individual to whom the identity information pertains; or by the authority of law. In cases where the individual has given his consent to the processing of identity information, state of the art operational methods and technologies must be applied and updated to ensure that the data is de-identified but re-identifiable for law enforcement purposes following proper procedures as set out by applicable law. If identity information is used for a Permitted Exemption, the Receiver is responsible for ensuring compliance with additional security and protection measures that may be set out by applicable law or competent authorities. Trust Framework Providers shall only permit Receivers to use sensitive identity information with the opt-in consent of the individual, except that sensitive identity information may be used without consent: - if the use is necessary in an employment relationship where adequate safeguards are in place; or - to protect vital interests where the individual is incapable of consenting; or - where the Receiver is a non-profit organization that the individual is in contact with provided that the sensitive identity information is not disclosed to third parties without the consent of the individual; - if the individual has made the sensitive identity information public; or - if necessary in connection with legal claims; or - if related to the provision of medical care or the management of health-care services by health professionals; or - when necessary for the performance of a task carried out in the public interest or by authority of law; or - when necessary for the purposes of the legitimate interests pursued by the Discloser or a Receiver provided the privacy interests of the individual are not disproportionably affected.

E. DATA QUALITY

	Public Policy (red font indicates intensification from previous level)
LOP1	Identity information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
LOP2	Identity information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
LOP3	Identity information must be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. Reasonable measures must be taken to ensure that information that is inaccurate or incomplete is erased or rectified.
LOP4	Identity information must be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. Reasonable measures must be taken to ensure that information that is inaccurate or incomplete is erased or rectified. Receiver will keep a log of all corrections, completions and deletions made and will create a retention schedule to formalize archive, destruction or anonymization procedures.

F. SECURITY SAFEGUARDS

	Public Policy (red font indicates intensification from previous level)
LOP1	Receiver should protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.
LOP2	Receiver should protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.
LOP3	Receiver must protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards must be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information and the context in which it is held, and must be subject to periodic review and reassessment.
LOP4	Receiver must protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards must be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information and the context in which it is held, and must be subject to periodic review and reassessment. When identity information is shared under a trust framework (as described in the white paper on "The Open Identity Trust Framework (OITF) Model", noted above in the main body of this paper), among other things the trust framework provider (TFP) must protect against the threats of: phishing; collusion; collusion coupled with real-time surveillance; inadequate transaction proof; impersonation; networks' being down; unauthorized token transfer; and user profiling.

G. RIGHT OF ACCESS / INDIVIDUAL PARTICIPATION

	Public Policy (red font indicates intensification from previous level)
LOP1	Individuals who have provided sufficient proof of their identity should be able to: (a) obtain from [Receiver] confirmation of whether or not [Receiver] holds identity information about them; (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. Such access and opportunity for correction should be provided except where: the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question; the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or the information privacy of persons other than the individual could be violated. If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.
LOP2	Individuals who have provided sufficient proof of their identity should be able to: (a) obtain [Receiver] confirmation of whether or not [Receiver] holds identity information about them; (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. Such access and opportunity for correction should be provided except where: the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or the information privacy of persons other than the individual could be violated. [Note: Unlike LOP1, there is no exception to the right of access and opportunity when the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question.] If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.
LOP3	Without constraint if requests are made at reasonable intervals, individuals who have provided sufficient proof of their identity must be able to: (a) obtain from the [Receiver] confirmation of whether or not identity information relating to him is being used and the circumstances of this use (such as purpose, disclosures, and source); (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted, with notification sent to third parties to whom the data have been disclosed of any measures taken, unless such effort would be disproportionate.[Note: Unlike LOP1 but like LOP2, there is no exception to the right of access and opportunity when the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, or to protect confidential commercial information.]If a request under (a) or (b) or a challenge under (c) is denied, the individual must be provided with reasons why and be able to challenge such denial.
LOP4	Without constraint at reasonable intervals, individuals who have provided sufficient proof of their identity must be able to: (a) obtain from the [Receiver] confirmation of whether or not identity information relating to him is being use and the circumstances of this use (such as purpose, disclosures, and source); (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted, with notification sent to third parties to whom the data have been disclosed of any measures taken, unless such effort would be disproportionate.[Note: Unlike LOP1 but like LOP2 and LOP3, there is no exception to the right of access and opportunity when the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, or to protect confidential commercial information.] If a request under (a) or (b) or a challenge under (c) is denied, the individual must be provided with reasons why and be able to challenge such denial. For trust frameworks, the trust framework provider (TFP) must ensure that assessors and auditors check that trust framework participants limit the Right of Access / Individual Participation only under Permitted Exemptions of the applicable law(s).

H. ACCOUNTABILITY

	Public Policy (red font indicates intensification from previous level)
LOP1	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. In trust frameworks, the trust framework provider (TFP) should ensure that participants apply operational and technological methods to give effect to data protection principles as specified for LOP1.
LOP2	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. In trust frameworks, the trust framework provider (TFP) should ensure that participants apply operational and technological methods to give full effect to data protection principles as specified for LOP2.
LOP3	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. In trust frameworks, the trust framework provider (TFP) must ensure that participants apply operational and technological methods to give full effect to data protection principles as specified for LOP3.
LOP4	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. If rights or obligations accompanying any data protection principle at LOP4 are restricted under a Permitted Exemption, the Receiver must notify relevant authorities. In trust frameworks, the trust framework provider (TFP) must ensure that participants apply operational and technological methods to give full effect to data protection principles as specified for LOP4.

I. ONWARD TRANSFER

	Public Policy (red font indicates intensification from previous level)
LOP1	When identity information is to be transferred to an independent third party, whether domestically or internationally, the Discloser should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently at the same LOP.
LOP2	When identity information is to be transferred to an independent third party, whether domestically or internationally, the Discloser should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently at the same or a higher LOP, taking all reasonable and appropriate steps to ensure that [cross-trust-framework] flows of identity information are uninterrupted and secure. Members of trust frameworks should avoid developing policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to cross-trust-framework flows of identity information that would exceed requirements for such protection.
LOP3	When identity information is to be transferred to another person or organization, whether domestically or internationally, the Discloser must obtain the consent of the individual or exercise due diligence and take steps (e.g., contractually) to ensure that the Receiver will protect the information consistently at the same or a higher LOP, taking all reasonable steps to ensure that [cross-trust-framework] flows of identity information are uninterrupted and secure. Members of trust frameworks should avoid developing policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to cross-trust-framework flows of identity information that would exceed requirements for such protection. Trust framework providers (TFPs) must operate a publicly available white list of trust frameworks that have been certified as offering adequate protection, with the specific LOPs indicated.
LOP4	When identity information is to be transferred to another person or organization, whether domestically or internationally, the Discloser must obtain the explicit consent of the individual or exercise due diligence and take steps to ensure that the recipient person or organization will protect the information consistently at the same LOP, taking all appropriate steps (*e.g.*, contractually) to ensure that [cross-trust-framework] flows of identity information are uninterrupted and secure. [Members of trust frameworks] should avoid developing policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to [cross-trust-framework] flows of identity information that would exceed requirements for such protection. Trust framework providers (TFPs) must operate a publicly available white list of trust frameworks that have been certified as offering adequate protection, with the specific LOPs indicated. For trust frameworks claiming to follow the Open Identity Trust Framework (OITF) Model (as spelled out in the white paper referenced above), TFPs must submit to oversight by a governance body that includes representatives of citizens of the relevant jurisdiction(s).

J. PERMITTED EXEMPTIONS

	Public Policy (red font indicates intensification from previous level)
LOP1	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted if they are permitted by applicable law or if they relate to national sovereignty; national security; public safety; and public policy. Any exemptions should be limited and proportional to meeting the objectives to which the exceptions relate and are either made known to the public or in accordance with applicable law.
LOP2	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted if they are permitted by applicable law or if they relate to national sovereignty; national security; public safety; and public policy. Any exemptions should be limited and proportional to meeting the objectives to which the exceptions relate and are made known to the public and in accordance with applicable law.
LOP3	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted when permitted by applicable law or if such a restriction constitutes a necessary measure : (a) to safeguard national security; (b) to safeguard defense; (c) to safeguard public security; (d) for the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) to safeguard an important economic or financial interest of [a sovereign], including monetary, budgetary and taxation matters; (f) for a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) for the protection of the individual or of the rights and freedoms of others; (h) to ensure that the privacy of persons other than the individual will not be violated. [Notes: The standard of "necessary" is stronger than that of "if they relate to" that is used in LOP1 and LOP2. Reasons are more specific here and do not include the general terms "national sovereignty" and "public policy" that are used in LOP1 and LOP2.] Any exemptions must be limited and proportional to meeting the objectives to which the exceptions relate and are made known to the public and in accordance with applicable law.
LOP4	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted when permitted by applicable law or if such a restriction constitutes a necessary measure: (a) to safeguard national security; (b) to safeguard defense; (c) to safeguard public security; (d) for the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) to safeguard an important economic or financial interest of [a sovereign], including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) for the protection of the individual or of the rights and freedoms of others; (h) to ensure that the privacy of persons other than the individual will not be violated. [Notes: The standard of "necessary" is stronger than that of "if they relate to" that is used in LOP1 and LOP2. Reasons are more specific here and do not include the general terms "national sovereignty" and "public policy" that are used in LOP1 and LOP2.] Any exemptions must be limited and proportional to meeting the objectives to which the exceptions relate and are made known to the public and in accordance with applicable law. If rights or obligations accompanying any data protection principle at LOP4 are restricted under a Permitted Exemption, the party claiming the exemption must document the following: (1) The specific Permitted Exemption claimed. (2) The reason(s) why it is being claimed. (4) A straightforward explanation of how the measure will be implemented technologically and operationally. (5) What mechanism or process will be put in place to ensure that the measure is not implemented in a way that is arbitrary or overly broad.

LEVEL OF PROTECTION 1

	Public Policy
Collection Limitation	Receiver may collect identity information if it is relevant to stated purposes (which may be very broad). Publicly available identity information is not subject to these limits. Receiver should obtain the identity information by lawful and fair means.
Notice	If the identity information is not already publicly available, Receivers should give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; and what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information. In terms of timing, Receivers should take all reasonably practicable steps to ensure notice is before or at time of collection, but if not then, as soon after as practicable.
Choice	Individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to opt out *of* the arrangement.
Use	Receiver should use identity information only (a) to fulfill the purposes of collection and other compatible or related purposes for which notice was provided; (b) when necessary to provide a service or product requested by the individual; or (c) as permitted by applicable law.
Data Quality	Identity information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
Security Safeguards	Receiver should protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.
Right of Access/ Individual Participation	Individuals who have provided sufficient proof of their identity should be able to: (a) obtain from [Receiver] confirmation of whether or not [Receiver] holds identity information about them; (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. Such access and opportunity for correction should be provided except where: the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question; the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or the information privacy of persons other than the individual could be violated. If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.
Accountability	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. In trust frameworks, the trust framework provider (TFP) should ensure that participants apply operational and technological methods to give effect to data protection principles as specified for LOP1.
Onward Transfer	When identity information is to be transferred to an independent third party, whether domestically or internationally, the Discloser should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently at the same LOP.
Permitted Exemptions	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted if they are permitted by applicable law or if they relate to national sovereignty; national security; public safety; and public policy. Any exemptions should be limited and proportional to meeting the objectives to which the exceptions relate and are either made known to the public or in accordance with applicable law.

LEVEL OF PROTECTION 2

	Public Policy
Collection Limitation	Receiver should limit the collection of identity information. Publicly available identity information is not subject to these limits. Receiver should obtain the identity information by lawful and fair means.
Notice	If the identity information is not already publicly available, Receivers should give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information; general practices and policies; and subsequent changes of purpose. In terms of timing, Receivers should give notice not later than at the time of data collection.
Choice	Individuals must be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to *opt out* of the arrangement.
Use	Receiver should use identity information only (a) to fulfill the purposes of collection and other compatible or related purposes for which notice was provided; (b) when necessary to provide a service or product requested by the individual; or (c) as permitted by applicable law.
Data Quality	Identity information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
Security Safeguards	Receiver should protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.
Right of Access/ Individual Participation	Individuals who have provided sufficient proof of their identity should be able to: (a) obtain [Receiver] confirmation of whether or not [Receiver] holds identity information about them; (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. Such access and opportunity for correction should be provided except where: the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or the information privacy of persons other than the individual could be violated. [Note: Unlike LOP1, there is no exception to the right of access and opportunity when the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question.] If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.
Accountability	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. In trust frameworks, the trust framework provider (TFP) should ensure that participants apply operational and technological methods to give full effect to data protection principles as specified for LOP2.
Onward Transfer	When identity information is to be transferred to an independent third party, whether domestically or internationally, the Discloser should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently at the same or a higher LOP, taking all reasonable and appropriate steps to ensure that [cross-trust-framework] flows of identity information are uninterrupted and secure. Members of trust frameworks should avoid developing policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to cross-trust-framework flows of identity information that would exceed requirements for such protection.
Permitted Exemptions	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted if they are permitted by applicable law or if they relate to national sovereignty; national security; public safety; and public policy. Any exemptions should be limited and proportional to meeting the objectives to which the exceptions relate and are made known to the public and in accordance with applicable law.

LEVEL OF PROTECTION 3

	Public Policy
Collection Limitation	Receiver must limit the collection of identity information to what is proportionate for the specific purposes for which identity information is used. Receiver must obtain the identity information by lawful and fair means.
Notice	Unless the identity information is subject to a Permitted Exemption regarding notice, Receivers must give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information; general practices and policies; subsequent changes of purpose; and whether the submission of information requested is obligatory or voluntary and possible consequences of failure to submit it. In terms of timing, Receivers must give notice not later than at the time of data collection. Notice requirements apply even when the relevant individual is not the Discloser, although some flexibility is allowed in terms of timing and in case offering notice would be overly burdensome.
Choice	Individuals must be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to *opt in* to the arrangement. Individuals have a right to object to the use of their identity information. This right may be exercised at any time and, if justified, the Receiver may no longer use the identity information concerned. Such requests will in any case be justified if the relevant individual opposes the use of his identity information for marketing purposes. Except in cases covered by applicable Permitted Exemptions, individuals have the right to oppose decisions being made about them which would significantly affect them based solely on automated processing of their identity information.
Use	Except in cases covered by Permitted Exemptions, Receiver may use identity information only: with the consent of the individual; to provide a service or product requested by the individual; when necessary for the performance of a task carried out in the public interest or by authority of law; or when necessary for the purposes of the legitimate interests pursued by the Discloser or a Receiver provided the privacy interests of the individual are not disproportionably affected. Trust Framework Providers shall only permit Receivers to use sensitive identity information with the opt-in consent of the individual, except that sensitive identity information may be used without consent: - if the use is necessary in an employment relationship where adequate safeguards are in place; or - to protect vital interests where the individual is incapable of consenting; or - where the Receiver is a non-profit organization that the individual is in contact with provided that the sensitive identity information is not disclosed to third parties without the consent of the individual; - if the individual has made the sensitive identity information public; or - if necessary in connection with legal claims; or - if related to the provision of medical care or the management of health-care services by health professionals; or - when necessary for the performance of a task carried out in the public interest or by authority of law; or - when necessary for the purposes of the legitimate interests pursued by the Discloser or a Receiver provided the privacy interests of the individual are not disproportionably affected.
Data Quality	Identity information must be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. Reasonable measures must be taken to ensure that information that is inaccurate or incomplete is erased or rectified.
Security Safeguards	Receiver must protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards must be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information and the context in which it is held, and must be subject to periodic review and reassessment.
Right of Access/ Individual Participation	Without constraint if requests are made at reasonable intervals, individuals who have provided sufficient proof of their identity must be able to: (a) obtain from the [Receiver] confirmation of whether or not identity information relating to him is being used and the circumstances of this use (such as purpose, disclosures, and source); (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted, with notification sent to third parties to whom the data have been disclosed of any measures taken, unless such effort would be disproportionate.[Note: Unlike LOP1 but like LOP2, there is no exception to the right of access and opportunity when the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, or to protect confidential commercial information.]If a request under (a) or (b) or a challenge under (c) is denied, the individual must be provided with reasons why and be able to challenge such denial.
Accountability	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. In trust frameworks, the trust framework provider (TFP) must ensure that participants apply

	operational and technological methods to give full effect to data protection principles as specified for LOP3.
Onward Transfer	When identity information is to be transferred to another person or organization, whether domestically or internationally, the Discloser must obtain the consent of the individual or exercise due diligence and take steps (e.g., contractually) to ensure that the Receiver will protect the information consistently at the same or a higher LOP, taking all reasonable steps to ensure that [cross-trust-framework] flows of identity information are uninterrupted and secure. Members of trust frameworks should avoid developing policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to cross-trust-framework flows of identity information that would exceed requirements for such protection. Trust framework providers (TFPs) must operate a publicly available white list of trust frameworks that have been certified as offering adequate protection, with the specific LOPs indicated.
Permitted Exemptions	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted when permitted by applicable law or if such a restriction constitutes a necessary measure : (a) to safeguard national security; (b) to safeguard defense; (c) to safeguard public security; (d) for the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) to safeguard an important economic or financial interest of [a sovereign], including monetary, budgetary and taxation matters; (f) for a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) for the protection of the individual or of the rights and freedoms of others; (h) to ensure that the privacy of persons other than the individual will not be violated. [Notes: The standard of "necessary" is stronger than that of "if they relate to" that is used in LOP1 and LOP2. Reasons are more specific here and do not include the general terms "national sovereignty" and "public policy" that are used in LOP1 and LOP2.] Any exemptions must be limited and proportional to meeting the objectives to which the exceptions relate and are made known to the public and in accordance with applicable law.

LEVEL OF PROTECTION 4

	Public Policy
Collection Limitation	Receiver must limit the collection of identity information to the minimum necessary for the specific purposes for which it is to be used, and Receiver must follow best practices for preventing correlation/the linking of transactions and re-identification. Receiver must obtain the identity information by lawful and fair means.
Notice	Unless the identity information is subject to a Permitted Exemption regarding notice, Receivers must give notice about: the fact that identity information is collected; purposes; types of onward transfer recipients; contact details for the Receiver; what kind of choices are offered for limiting use and disclosure and for accessing and correcting identity information; general practices and policies; subsequent changes of purpose; whether the submission of information requested is obligatory or voluntary and possible consequences of failure to submit it; and the security safeguards. In terms of timing, Receivers must give notice not later than at the time of collection. Notice requirements apply even when the relevant individual is not the Discloser, unless such notice would be impossible because of applied protection measures (de-identification measures). If identity information is disclosed under a trust framework, the trust framework provider (TFP) must ensure that there is a publicly accessible registry of participants and their practices with respect to the specific interactions that take place under that trust framework. (See the white paper on "The Open Identity Trust Framework (OITF) Model", noted in the main body of this "Levels of Protection" paper.)
Choice	Individuals must be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their identity information. This requirement does not apply if the identity information is already publicly available. The default is to be set so that the user must take action if he wishes to *opt in* to the arrangement. Individuals have a right to object to the use of their identity information. This right may be exercised at any time and, if justified, the Receiver may no longer use the identity information concerned. Such requests will in any case be justified if the relevant individual opposes the use of his identity information for marketing purposes. Except in cases covered by applicable Permitted Exemptions, individuals have the right to oppose decisions being made about them which would significantly affect them based solely on automated processing of their identity information. Where applicable law requires and the state of the art enables such implementation, the Receiver shall enable individuals to take data that they have contributed in one context and bring ("port") it to different contexts as the individual desires. Where applicable law requires and the state of the art enables such implementation, the Receiver shall follow best practices to allow individuals easily to set default preferences for the treatment of their identity information.
Use	Except in cases covered by specific Permitted Exemptions, Receiver may use identity information only: with the explicit consent of the individual; when necessary to protect the vital interests of the individual to whom the identity information pertains; or by the authority of law. In cases where the individual has given his consent to the processing of identity information, state of the art operational methods and technologies must be applied and updated to ensure that the data is de-identified but re-identifiable for law enforcement purposes following proper procedures as set out by applicable law. If identity information is used for a Permitted Exemption, the Receiver is responsible for ensuring compliance with additional security and protection measures that may be set out by applicable law or competent authorities.
Data Quality	Identity information must be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. Reasonable measures must be taken to ensure that information that is inaccurate or incomplete is erased or rectified.
Security Safeguards	Receiver must protect identity information that it holds with appropriate safeguards against risks, such as loss or unauthorized access to identity information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Having regard to the state of the art and the cost of their implementation, such safeguards must be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information and the context in which it is held, and must be subject to periodic review and reassessment. When identity information is shared under a trust framework (as described in the white paper on "The Open Identity Trust Framework (OITF) Model", noted above in the main body of this paper), among other things the trust framework provider (TFP) must protect against the threats of: phishing; collusion; collusion coupled with real-time surveillance; inadequate transaction proof; impersonation; networks' being down; unauthorized token transfer; and user profiling.
Right of Access/ Individual Participation	*Without* constraint at reasonable intervals, individuals who have provided sufficient proof of their identity must be able to: (a) obtain from the [Receiver] confirmation of whether or not identity information relating to him is being use and the circumstances of this use (such as purpose, disclosures, and source); (b) have communicated to them identity information about them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted, with notification sent to third parties to whom the data have been disclosed of any measures taken, unless such effort would be disproportionate.[Note: Unlike LOP1 but like LOP2 and LOP3, there is no exception to the right of access and opportunity when the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, or to protect confidential commercial information.] If a request under (a) or (b) or a challenge under (c) is denied, the individual must be provided with reasons why and be able to challenge such denial. For trust frameworks, the trust framework provider (TFP) must ensure that assessors and

	auditors check that trust framework participants limit the Right of Access / Individual Participation only under Permitted Exemptions of the applicable law(s).
Accountability	Where applicable law requires, the individual shall be notified of any data loss or breach of his or her identity information. If rights or obligations accompanying any data protection principle at LOP4 are restricted under a Permitted Exemption, the Receiver must notify relevant authorities. In trust frameworks, the trust framework provider (TFP) must ensure that participants apply operational and technological methods to give full effect to data protection principles as specified for LOP4.
Onward Transfer	When identity information is to be transferred to another person or organization, whether domestically or internationally, the Discloser must obtain the explicit consent of the individual or exercise due diligence and take steps to ensure that the recipient person or organization will protect the information consistently at the same LOP, taking all appropriate steps (e.g., contractually) to ensure that [cross-trust-framework] flows of identity information are uninterrupted and secure. [Members of trust frameworks] should avoid developing policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to [cross-trust-framework] flows of identity information that would exceed requirements for such protection. Trust framework providers (TFPs) must operate a publicly available white list of trust frameworks that have been certified as offering adequate protection, with the specific LOPs indicated. For trust frameworks claiming to follow the Open Identity Trust Framework (OITF) Model (as spelled out in the white paper referenced above), TFPs must submit to oversight by a governance body that includes representatives of citizens of the relevant jurisdiction(s).
Permitted Exemptions	Exemptions to the principles of Collection Limitation, Notice, Use, Data Quality, and Right of Access/ Individual Participation are permitted when permitted by applicable law or if such a restriction constitutes a necessary measure: (a) to safeguard national security; (b) to safeguard defense; (c) to safeguard public security; (d) for the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) to safeguard an important economic or financial interest of [a sovereign], including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) for the protection of the individual or of the rights and freedoms of others; (h) to ensure that the privacy of persons other than the individual will not be violated. [Notes: The standard of "necessary" is stronger than that of "if they relate to" that is used in LOP1 and LOP2. Reasons are more specific here and do not include the general terms "national sovereignty" and "public policy" that are used in LOP1 and LOP2.] Any exemptions must be limited and proportional to meeting the objectives to which the exceptions relate and are made known to the public and in accordance with applicable law. If rights or obligations accompanying any data protection principle at LOP4 are restricted under a Permitted Exemption, the party claiming the exemption must document the following: (1) The specific Permitted Exemption claimed. (2) The reason(s) why it is being claimed. (4) A straightforward explanation of how the measure will be implemented technologically and operationally. (5) What mechanism or process will be put in place to ensure that the measure is not implemented in a way that is arbitrary or overly broad.