Trust Framework System Rules for Personal Data and Individual Identity Services

Legal Notices

Attributions and Disclaimer: This work is based upon work supported by the Defense Advance Research Project Agency (DARPA) and Space and Naval Warfare Systems Center Pacific under Contract N66001-11-C-4006. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Advance Research project Agency (DARPA) and Space and Naval Warfare Systems Center Pacific.

Document Information: Version 1.06; June 20, 2013; Comments to: daz@media.mit.edu; Authoritative stable release version of the System Rules is published at the MIT Human Dynamics Lab openPDS project site: http://openpds.media.mit.edu/#rules; The System Rules project background and news site: http://ecitizen.mit.edu/modelrules; The current exploratory drafts and alternative provisions under consideration in the MIT Human Dynamics Lab GitHub Repository: https://github.com/HumanDynamics/SystemRules

Preface

This document provides Trust Framework System Rules[1] for the provision of Personal Data and Individual Identity services. The architecture and model followed by these System

Rules enables interoperability at the business, legal and technical dimensions, and ensures that each of those dimensions is expressly aligned, harmonized, and integrated.

Specifically, these System Rules anticipate and are tailored to support a prospective production grade roll out of openPDS and Funf software for Reality Analysis, and more generally, as an example of how System Rules following this model can enable and accelerate achieving the broader goal of a Personal Data Ecology. Please note that for purposes of presenting a complete and coherent reference example, "placeholders"[2] and "hooks[3]" have been used for names of parties or business services. For future commercial or production grade use of these Rules, implementers would replace the example parties, service descriptions, etc., with the respective names and applicable terms specific to the business roles and relationships agreed among the parties.

1. BUSINESS RULES[4]

1.1 Scope and Purpose

These System Rules apply to the use of the Personal Data and Individual Identity System by Individual Users, Third Party Service Providers and the System Provider, individually and in any combination. These Rules are intended and shall be interpreted to ensure that the access and interoperability enabled for access to and sharing of personal data is at all times subject to privacy protection and fair information practices.

The purpose of the System is to enable a means for individual human beings to simply, efficiently, securely and effectively exercise their rights to store and keep private their own personal data and to share access to such data by their express consent and authorization through System Services. The System is specifically intended to empower individual users to not only grant or not grant such authorizations, but also to monitor, manage and modify or revoke such access over time. The simple, efficient, secure and effective Personal Data Services are also intended to enable Third Party Service Providers to provide added value to individual Participants and derive value from access to permission-based data access in an expanded marketplace. Leveraging the capability of API's for Third Party apps under a common rule set and services enhances the value of the system to all parties while ensuring privacy.

The issuance of individual identity credentials and related System Services is likewise intended to empower individual Participant rights and expectations of autonomy and control of their own digital identity. The information comprising the digital identifiers, attributes, tokens and other similar identity data is also considered personal data of a particularly sensitive and valuable nature, hence a compatible and beneficial set of Services to be included within this System and subject to these Rules[5].

The focus of these Rules is to standardize essential interface and interoperability implementation requirements necessary to ensure expected outcomes by all Parties while

encouraging wide latitude for individually agreed interactions and competitively evolving innovation. These System Rules are intended to provide a reliable and efficient method of achieving the purpose of the System.[6]

1.2 Parties and Roles

These System Rules are applied by and to the Parties registered as current Participants in the System Registry. Each Party, in order to be approved as a Participant, must contractually assent to the Participation Agreement, including the Terms of Agreement corresponding to the Role or Roles that Party will conduct within the System and specifically including acceptance of the rights, obligations and functions allocated to the Role or Roles agreed by each Party:

1.2.1 Individual Participant

An individual human being who has contractually assented to Terms of Agreement and is a customer holding a valid account with the Personal Data Store. An Individual Participant may use his or her account to request, accept and use a Grant of Authorization to access the Personal Data of another Principal Participant user.

Any individual human who contractually assents to the Terms of Agreement is eligible to apply for and hold an Account on the System. Services or other premium functions offered on a subscription, one-time fee or other billing basis are available subject to fulfillment of applicable payment terms as agreed by the Individual User.

1.2.2 Principal Participant

An individual human who has contractually assented to Terms of Agreement and is a customer holding a valid account with the Personal Data Store offered by the System Provider under these Rules. A Principal Participant may use his or her account to store his or her own Personal Data on the System and to Grant Authorization for accessing that Personal Data to Third Party Service Providers and/or to individual Participants.

1.2.3 System Provider

The Party or Parties responsible for the Personal Data System, comprised of the Personal Data Store and Services. The System Provider promulgates these System Rules.

1.2.4 Third Party Service Providers

The Party or Parties that operate and provide Third Party Services approved for use with the System and in accordance with these Rules. Only Third Party Providers that have been approved by the System Provider and contractually assented to the Participation Agreement, including the Terms of Agreement, are eligible to Participate in the System. Only an Approved Third Party Service Provider is eligible to receive the tokens necessary to use a Grant of Authorization by an Individual User or otherwise to use an Approved

Scope and Grant Type for access of any kind to data or other resources within or through the System or otherwise subject to these Rules.

1.3 System Services

1.3.1 Service Lifecycle

Approval by the System Provider is required as a precondition to the offering of any Service though this System. Any approved Service that is currently offered through the System is enumerated in Rule 1.3.2 and is available in accordance with the technical specifications defined under Rule 3.2 and subject to all relevant Rules and used subject to the relevant provisions of the Terms of Agreement of any Participant using the Service.

1.3.2 System Service

The following Services are approved and provisioned for use by or with the System, subject to these Rules:

1.3.2.1 "Personal Data Storage and Archive" services,

1.3.2.2 “Personal Data Collection and Import” services,

1.3.2.3 "Personal Data Sharing Control" services,

1.3.2.4 “ Analytics and Visualization" services, and

1.3.2.5 “Personal Data Export and Deletion” services.

1.4 Recording and Reporting

Any Recording or Reporting requirement under these Rules must result in the logging of the required record at the System Registry (or other facility provided by the System Provider) within the time prescribed or if no time is prescribed or if extenuating circumstances are permitted under these Rules, it shall be logged as soon as practicable.

Every Third Party Service must be implemented so as to ensure creation, accuracy, integrity, preservation and accessibility of Required Records such that upon review an objectively verifiable account can be made of the relevant transactions or other actions, the salient terms (i.e. the data accessed, modified or deleted or other essential terms) the parties involved, the relevant times, and the applicable Terms of Agreement and Terms of Authorization.

1.5 Use of System Logo and Marketing

Any use of the System Logo, and any marketing, advertising or other public communications referencing approved Third Party Provider status or other affiliation with

this System is prohibited unless explicitly permitted in the applicable Terms of Agreement and only for such time as the Terms of Agreement are in effect.

2. LEGAL RULES

2.1 Scope and Application

2.1.1 Promulgation of Rules

The content comprising the "System Rules" duly promulgated by the System Provider in accordance with these Rules, is the formal and binding normative version of these Rules as of the moment of publication and until the moment of publication of a subsequent version or for such period of time as provided under these Rules.

2.1.2 Order of Precedence

In the event of a conflict between the provisions of these Rules and the provisions of the Terms of Agreement between any Parties to these Rules, then the provisions of these Rules shall prevail.

In the event of a conflict between the terms of these Rules and an Independent Commercial Contract between any Parties to these Rules, then, as between a Principal Participant and a Third Party Service Provider, the provisions of the applicable Terms of Authorization incorporated by reference into the Parties Terms of Agreement shall prevail, and otherwise the provision of the Independent Commercial Contract shall prevail.

2.2 Rights and Obligations of Participants

2.2.1 General Obligation

All Participants agree to abide by the terms and act in accordance with these Rules and adhere to respect each Principal Participant's ownership and control rights to their own Personal Data stored in or accessible through this System.

2.2.2 Protection and Promotion of Individual Participant Identity and Data Rights

The System Provider is responsible for safeguarding the Individual Participant's elemental rights to his or her own individual identity and ownership of their personal data and may as appropriate protect and defend such rights and as needed represent the interests of such Participant vis-a-vis external parties when such rights are threatened.

2.2.3 Minimum Required Obligations of Third Party Providers to individual Participants

Each Third Party Provider agrees to comply with the Terms of Authorization between itself and each individual Participant from whom the Third Party Provider has received a Grant of Authorization for access to personal data of such Participant

To ensure the purpose of this System and expectations of individual Participants are met, every Third Party Provider must correctly and completely implement the Approved Scopes and Grant Types and corresponding obligations and stipulations for each such Scope and Grant. Furthermore, every Third Party Provider must agree to accept that the legal rights and obligations corresponding to each Approved Scopes and Grant Types are contractually enforceable by the Participant that has granted such Authorization to such Third Party Provider or by the System Provider as a Third Party Beneficiary. Failure to comply with these requirements renders any Third Party Provider ineligible for Participation and subject to termination, suspension, or a review process at the sole discretion of the System Provider.

To be eligible for approval by the System Provider, a prospective Third Party Provider must submit a Third Party Provider Application, including truthful, accurate and complete information. Every Third Party Provider must contractually assent to abide by and in practice adhere to these Rules. Manual Registration of a Third Party Service, Client or Other App is required. Any approved Third Party Provider may accept individual Participant Grants of Authorization corresponding to one or more Approved Scope and Grant Type for access to that Participant's Personal Data.

Any approved Third Party Provider may establish such additional terms of service, including with respect to billing, liability and service quality, with individual Participants of the System, as the parties may agree provided that no contractual term or other obligation shall be enforceable against any individual Participant to the extent the obligation arises from or applies to that Participant 's Grant of Authorization to the Third Party Provider and is inconsistent with any provision of these Rules.

2.3 Logging and Reporting

2.3.2 Recording With System Registry

The Required Record of any transaction or other action subject to a Reporting requirements under Rule 1.4 or otherwise required under these Rules must be logged with the System Registry (or other facility provided by the System Provider) and a copy preserved by the Party responsible. The following actions are subject to a logging requirement:

- Promulgation and Amendment to these Rules
- Activation, Status Change or Closure of Participant Account
- Each Grant of Authorization by a Principal Participant, including Modification or Revocation of Such Grant of Authorization
- Supported Scopes of User Authorization, Including Modification or Removal of such Scopes

- System Interfaces for REST calls, including Modification or Removal of any Such Specification
- Provision, Modification or Removal of a System Service or Component

2.4 Liability and Indemnification

Under these Rules, no Individual User shall be liable to nor shall owe any obligation of indemnity to any other party for any actions that were conducted in compliance with these Rules. The applicable provisions of the Terms of Agreement regarding liability, indemnity, damages and warranties shall apply to Parties to such agreements, subject to the Order of Precedence defined in Rule 2.1.2.

2.5 Intellectual Property

2.5.1 Trademark and License in System Trustmark and Logo

Use of the System trademarks or logos must comply with the Trustmark and Branding Policy and License Agreement. No Party may use or display any trademark or logo without explicit permission and license to do so. Parties that are engaged in a process of applying for participation are not parties to the License Agreement and not permitted to use such trademarks or logos. Parties that were Participants at one time but whose Participation status is suspended or terminated, whether voluntarily or involuntarily, are likewise not permitted to use or display the System trademarks or logos, and must cease any use that had previously been permitted in accordance with the license terms.

2.5.2 Copyright and License in System Rules

These Rules are available to be downloaded, stored, transmitted and duplicated on a royalty free, perpetual and global basis, under a Creative Commons Attribution-Share Alike 3.0 Unported License. The System Provider shall ensure the Creative Commons license is applied to these Rules.

2.6 Amendment

These Rules may be amended from time to time by the System Provider in accordance with the Notice requirements of Section 2.7.

2.7 Notice

Amendment of a Rule or change to the System that is not material is effective when duly promulgated by the System Provider. An affected Participant is entitled to receive 30 calendar days advance notice of any amendment of a Rule or change to the System that constitutes material change, unless an emergency condition requires a shorter period or no notice.

2.8 Other Legal Terms

The Terms of Agreement, including the Terms of Authorization, as executed or adopted by each Participant include more specific terms and may include varying provisions, subject to Rule 2.1.2 governing Order of Precedence. The terms defining and governing the overall business relationship and legal rights, expectations or other responsibilities and duties of the Participants are addressed in one or more Independent Commercial Contracts executed or adopted by Participants, subject to Rule 2.1.2.

3. TECHNICAL RULES

3.1 Scope and Application

3.1.2 Supported Standards

The System supports and depends upon the following Standards and relies upon conformance with and interoperability based upon correct implementation of these standards:

3.1.2.1 OAuth2

The System Authorization and Resource servers support the final version of the AUth2 Core as defined at http://tools.ietf.org/html/draft-ietf-oauth-v2

The System Authorization and Resource servers support the final version of the AUth2 Bearer Token usage as defined at Bearer: http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer

3.1.2.4 Authoritative Normative Sources

OAuth2:
Core: http://tools.ietf.org/html/draft-ietf-oauth-v2
Bearer: http://tools.ietf.org/html/draft-ietf-oauth-v2-bearer

JSON Object Signing and Encryption:
JWT (tokens): http://tools.ietf.org/html/draft-ietf-oauth-json-web-token
JWS (signing): http://tools.ietf.org/html/draft-ietf-jose-json-web-signature
JWE (encryption): http://tools.ietf.org/html/draft-ietf-jose-json-web-encryption
JWK (keys): http://tools.ietf.org/html/draft-ietf-jose-json-web-key
JWA (algorithms): http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms

3.2 Service Provision and System Components[7]

Services offered through the System are enumerated in Rule 1.3.

3.2.1 Personal Data services

A Principal Individual User may import Personal Data and other records to their Personal Data Store that is hosted at the OpenPDS operated by System Provider by use of a Third Party Provider that has an approved service for that transaction.

3.2.2 System Components

In addition to Services and Interfaces, the System includes the following modular components.

3.2.2.1 openPDS

The authoritative version and build of openPDS software supported and implemented in the System under these Rules is located at https://github.com/humandynamics.

3.2.2.2 Funf Mobile Sensor Framework

The Mobile Health Funf Mobile Sensor Framework is open source software available for inclusion in Android apps available for use by Principal Individual Users. The specifications of the current supported version and build of this software and links to documentation is available at http://funf.org.

3.3 Approved Scopes of User Authorization and Grant Types

Only requests for access to Personal Data that conform with the defined Approved Scopes and Grant Types are permitted or supported under these Rules.[8]

3.4 Security and Resilience[9]

Passwords: Only an Individual User's Account password can decrypt that user's Personal Data or other sensitive information, and System Provider does not store this password. As a result, no one—not even System Provider employees—can see the sensitive information a Principal User places in the System. If a Principal User forgets his or her password and needs to reset it, the System Provider shall delete that user's sensitive information for his or her own protection. System Provider must also have mechanisms in place to stop brute force attacks on passwords, and offer multi-factor authentication and secure password recovery

Servers: Personal Data is stored in a major U.S. server storage facility that has 24/7 security guards and biometric security for entry, has been issued an SSAE16 Type II SOC 1 Report, is a PCI Security Standards Council Member, is Safe Harbor Certified, and offers protection via firewalls, its own intrusion detection systems, and other measures.

Data Storage: All personal data are encrypted in database servers, including by the use of 256-bit AES encryption and RSA 2048 asymmetric key encryption. Personal Data containing sensitive information must be encrypted uniquely, in order to add an extra layer of security. Non-sensitive information may only be accessed through a Principal User-chosen password that must not be stored by the System Provider. While technically possible for a small and limited group of System operations employees to access non-sensitive information, they are strictly forbidden from doing so, consistent with System Provider policies and these Rules, unless required by law, and access to System Provider servers is carefully logged.

Secure Coding and Data Management Practices: System Provider shall not use insecure third-party delivery networks, and must ensure that Principal User Personal Data is never exposed. System Provider is not permitted to see Principal User Personal Data even in the context of crash reports. In addition, System Provider must not use data de-duplication methods, which can raise security and privacy concerns.

Security Testing and Certificates: System Provider conducts audits of System security, including penetration testing by outside firms. System Provider uses SSL certificates from VeriSign and GeoTrust. In addition, System Provider constantly monitors the System for potential threats and vulnerabilities.

Principal's Control Their Personal Data: Only a Participant account holder can grant individuals, companies or applications access to his or her Personal Data and permanently delete or export his or her Personal Data. Third Party Providers are not allowed to track Participants while they are on the System, and the System Provider does not track Participants when they leave the System or a mobile app that is part of the System.

System Provider Employees: All System Provider employees undergo background checks going back 10 years as a condition of employment, and all technical employees receive security training.

3.5 Testing and Change Management

The System makes available a sandbox and test harness to Third Party Provider applicants to test the readiness for business, legal and technical interoperability with other Participants and for Participants to text readiness of modified or new Services, Transactions or other functions.

Commentary

[1] These System Rules provide a model for future production grade roll out of the Personal Data Store and related services developed by the MIT Media Lab's Human Dynamics group. The approach of the System Rules is intended to enable the use of the Android Funf and openPDS software to collect and share behavioral information effectively while ensuring best practices for privacy protection and user-centered control and consent for sharing of personal data. The System Rules cover the roles, relationships, rights, and responsibilities of parties who are individual users of the openPDS software and services and parties that provide the Personal Data Store as well as additional approved third party providers of services or apps.

The approach is designed to be extensible to include additional types of technologies and services without need to change the basic model or method for using the Rules and therefore to be useful for future evolution of the openPDS and Funf software as well as for the reality analysis and personal data ecology research and development work of the MIT Media Lab Human Dynamics group more generally.

Please note that for purposes of presenting a complete and coherent reference example, "placeholders" and "hooks" have been used for names of parties or business services. For future commercial or production grade use of these Rules, implementers would replace the example parties, service descriptions, etc., with the respective applicable names or terms.

These System Rules are tailored to be directly usable and adoptable by existing personal data stores providers but also to adaptively scale in support of emerging big data marketplaces and personal data ecosystems. The increasing value, volume, velocity and variety of transactions flowing through web-based applications today are straining the current models and architecture to the breaking point. While the technology exists to push bandwidth and meter usage in various ways, current business and legal foundations are inadequate to establish trustworthy interoperability and predictable legal outcomes for desired personal data services and transactions. This draft provides a novel approach to address these needs, with a mix of standard reusable rules and agreements and a set of modular, extensible, and interoperable individual rules and components.

Personal data, as an asset class, will exist in networks, systems, markets, stores, services and transaction types that are at once very secure and very open, simultaneously high velocity and high volume, and both dynamically evolving and reliably predictable. The business models and relationships defining the scope and substance of transactions and services require a much more robust yet simple to apply set of legal and technical tools to adaptively design and deliver deals and lines of business. The legal agreements reflecting granular grants of authorization and governing vast numbers of globally distributed parties

require service oriented systems of rules and a data-driven contract infrastructure connecting all parties. The demands to rapidly deploy new architectures and services, maintain high levels of performance and reliability while also ensuring tight and responsive security, oversight, controls and response measures across the network, systems, applications, data and extended enterprise, in turn demand modularity, interoperability and resilience of technology that are all but unprecedented. However, there are today small pockets of best practices and exemplars of personal data and individual federated identity. These early instances provided the design patterns underlying the Model System Rules.

A key concept underlying these Model Rules is that the rules and corresponding agreements exist within a broader context and apply to parties that frequently also have existing commercial relationships and business arrangements. The Rules anticipate and support this fact through the "Trust Stack" approach, which anticipates the Rules being "layered" on top of existing business or other "trusted relationships" but not conflicting with or replacing the existing commercial contracts and other arrangements of the parties. This is fundamental to the design and intended use of the Model Rules and is a key way this approach can ensure true interoperability at the business and legal levels while being adoptable for a wide variety of different business models and commercial or other relationships. Model Rules deliberately stop short of assuming, much less insisting upon, presumed business models or methods, posited legal rights or responsibilities, or particular technical services or standards.

The way this plays out in the instance of these Model Rules for Personal Data Store Account Holders and Service Providers is two-fold. First, it is expected that the Third Party Service Providers will have independent "Terms of Service" with any "Participant" of the Personal Data System and that the "Terms of Authorization" are supplemental to those underlying business contracts. Second, it is similarly assumed that the System Provider will have deeper and more complex and broadly scoped business contracts with Third Party Service Providers, such as the "Developer Agreements" or "API Access Terms" or other commercial app market access terms. Therefore, the "Participation Agreement" between the System Provider and the Third Party Service Provider is designed to layer on top of that contract and not to conflict with or replace it. The specific terms that are common to the standardized, modular and scalable Model Rules are focused on the subset of issues and common needs for cross-boundary secure data sharing and not focused on the highly idiosyncratic commercial fee structures, service levels and other business model related aspects of a given implementation. In this way, the Model Rules can be used by a variety of different businesses and in many contexts and still allow many parties to have confidence that certain key issues are clearly addressed by any other parties that use and apply the Model Rules.

[2] Within this document, some content is explicitly intended as illustrative examples of potential ways the current research program could be rolled out in commercial or other production offerings, such as the particular types of data services and the specific work flow and interchange specifications between interoperating parties. Placeholder business

capabilities, legal relationships and technical functions serve as examples of the ways these integrated systems can be configured and how parties can structure and represent those implementations within the construct of these model system rules and agreements. Placeholder content is identified and discussed in this supplemental guidance and commentary addenda.

[3] The hooks are designated by words or phrases within highlighted [brackets] and that are presented in their intended final form, requiring only insertion of the specific identifiers or other names or information indicated, such as the legal name of a party or the URI or URL of a defined online resource such as, for example, a policy document or the interface for a directory entry or other database record.

[4] As applied to multiparty consortia or systems of systems, these System Rules would include many sets of terms not present to cover the postulated use case of a single company providing a PDS. To the extent multiple PDS and affiliated analytics or other personal data related service companies banded for the purpose of joining a network with high regard for and protections of personal control and superior capabilities for interoperability and scaling, these Rules could easily be adapted to their case. Among other things, more terms in all three sections would be required, potentially including in the business section new provision for such functions as: Operational and Financial Practices, Points of Contact, Invoicing and Billing, Support Coordination and Escalation, Business Continuity and Change Management.

[5] Please note the current version of this document does not directly include OpenID Connect or similar identity services, so as to focus attention on the Personal Data related service set. Generally, the combination of federated individual identity services and personal data services are complimentary and to some extent blur together in practice with respect to private or sensitive identity-related attributes. The services of personal data management and identity management are, however, severable and can be expressed in a modular fashion at the business, legal and technical dimensions of a system.
[6] The business scope and intended scenarios of use have been somewhat generalized to provide a flavor and example how these System Rules can be applied to personal data stores and services generally. The mobile health and other user testing and research on the DARPA project will not require a sophisticated set of rules.

In larger scale and more complex systems, it may be necessary to literally agree upon a set of Use Cases that are more detailed than the general intended scenario and which can serve as a tool to help the governing body membership identify the actual requirements and constraints applicable or desirable for the System. The substance and scope of the System as well as the requirements and rules for the parties can be detailed based on the general contours and content of the scenario. The method used to develop accurate and aligned business, legal and technical System Rules involves eliciting the business roles, functions, flows, roles, relationships, legal parties, transactions, rights, responsibilities, technical actors, actions, interactions, standards, security and other relevant input from the appropriate executives or other staff at the organization (or organizations) deploying a

personal data system, resulting in a more complete and adoption-ready launch and operation. For purposes of this draft set of System Rules, the business, legal and technical context and usage are based upon composites of existing common approaches and practice in general use and use the MIT openPDS software, social health analysis, and other features as key reference points.

[7] When applied to multiple PDS providers, this section would include a required minimum set of "Core Services" to be provided by any PDS operator within the System and an optional set of "Extended Services" that have been approved for provision within the System and are supported with some level of shared infrastructural shared services. This approach allows a more sophisticated and flexible result whereby services that are not approved but are not prohibited under the Rules (due to violation of a business legal or technical requirement) may also be offered by PDS providers but would not be listed in this section or supported by the Rules or the System.

[8] Formal publication of the "Approved Scopes and Grant Types" is one of the key ways that these System Rules ensure business, legal and technical interoperability and therefore a more reliable basis for providing predictable results. These Scopes are uniquely capable of harmonization and integration of the business, legal and technical context and are therefore elevated as a cornerstone of this architecture. The decision to allow a given type of third party service is fundamentally a strategic and executive business judgment. Such access is enabled by these Scopes and therefore is a direct manifestation of the intended business case. Similarly, defining, enabling and managing the grants of permission, consent or other authorization by the customers of a business is profoundly legal in nature. And the technical aspects of supporting Scopes and Grant Types is existentially a technical and information security matter, implementing complex standards and profiles and carefully sequences exchange protocols among a variety of systems and parties. Providing these business value propositions through integrated contractual code and technical code can not only enable higher quality and more competitive market offerings but is also essential to ensuring the privacy and control of Participants over their personal data.

[9] Security envisioned for commercial offering and production grade operations of the System has been benchmarked, by permission of, the best practices of premier personal data store provider Personal.com.