The Value of OIXnet

A New Registry for Online Trust

By Hal Warren

The Value of OIXnet

By Hal Warren

Today as never before, we have access to a wealth of digital attributes and sensor data that we control. What is missing, however, is the ability to easily manage these diverse silos of data. Identity and service providers could create higher-value content for business applications by aggregating these data in machine- or human-readable form. The **OIXnet Registry** is an early step in producing a registry service, a public database for Identity Providers (IdPs) to be registered, published and searched, and where they can make known to users the characteristics of the attributes they manage. It is then at the discretion of the identity owners to aggregate or disaggregate their personal data.

Imagine, for example, several years from now experiencing a sudden pain in your abdomen. Instead of debating whether to to take some antacid or set up a doctor's appointment, you instead head to a user-friendly diagnostic kiosk (we can call it "Watson"), set up in a private room at your local pharmacy. There, Watson requests access to your medical records, which includes multiple sources such as dental, chiropractor, and psychotherapist, and spans your lifetime. You have the option of granting one-time access. Next, Watson requests access to 3 months of your consumption data, which includes grocery and restaurant purchases if available. Again, you provide one-time access. Watson then asks for an image of your tongue and fingernails. You stick your tongue out at the camera and hold up your hands. Finally, Watson asks for a small blood sample, so you put your finger on the designated spot and experience a small pain prick.

Watson then says, "Based on the data, it appears that you may have a rare stomach disorder which could be life threatening. You should proceed immediately to the hospital emergency room for treatment. Would you like for us to transfer these findings to the local hospital so they can expect you? And will you share your geolocation with them until you arrive?"

You answer "Yes" and, when you pull up to the hospital, they are already expecting you and your insurance has been verified. You are admitted to a treatment room where a physician reviews and confirms the findings of Watson and you begin the necessary treatment for the stomach disorder.

Or, perhaps Watson determines that you simply have indigestion, in which case he directs you to aisle 3 and recommends an antacid, noting that if you are not feeling better within an hour to come back .

This potential future depends on trust in systems to provide and protect human attributes. In this case, we define "human attribute" as any behavior or characteristic recorded about you or any relationship you have with objects in the Internet of Things. The ability to use your online attributes depends on IdP requirements, your trust in their accuracy and an understanding of your rights in controlling their distribution.

Not all of your activities are under your control. For example, your driver's license number links to a record of your traffic violations. When you give this number to an auto insurance company, they are then privy to your driving history, which they use to determine your rates. While you decide who has access to your driver's license number, you are not able to obtain insurance or rent a car without providing it and, consequently, access to your driving record.

Online human attributes can be classified as **health, financial, consumption, contribution** or **biometric** over time. Each attribute type has different needs for protection and agility.

Suddenly awash in sensor data that we control, we have new capacity to organize information to our advantage. Smart phones can track where we are, at what altitude, and at what temperature through connection to nearby sensors. And at any point of our choosing, a panoramic photographic record of the moment can be shared with family and friends.

We cannot ourselves sense changes in barometric pressure, although sudden changes in pressure can have an impact on our experience of pain. Now with personal sensors for barometric pressure we can be informed by our mobile devices at the time these changes occur, with recommended courses of action for our specific condition and location.

Now, through wearable devices, suddenly we have access to biological measures of sleep and physical activity. Mobile apps, based on these data, inform and encourage us to become more active and responsible in what we do and eat. We can share this information with friends and "challenge" each other to help improve our results.

Missing is the ability to manage our silos of individual sensor data with ease. A registry of human attributes that provides basic IdP provenance and attribute types contained in the identity advances our online identity infrastructure and trust. Simple indication of whether the data contained in the identity is **private**, **commercial** or **public** provides machine reasoners the ability to make better connections on our behalf. Our personal computing devices become **serendipitous recommendation engines** over which we feel more control.

The Internet as we know it is the product of a registry. Domain Name Services (DNS), the global registry for domain names, made the World Wide Web possible by connecting machine names (www.domain) with Web servers (machines), identified by IP numbers. DNS also provides human contact information for domains which can be used by network engineers when problems arise.

Similarly, **OIXnet** is a new registry for online trust in human attributes produced by different IdPs. Self assertions made by IdPs are backed by legal liability that the claims are legitimate.

Born Semantic as Structured Data

The OIXnet Registry record starts with basic IdP demographics, contacts, protocols used and attribute characteristics stored. Following the structure promoted by the World Wide Web Consortium (W3-C), OIXNet records are presented as Uniform Resource Identifiers (URIs) to make transparent assertions on URLs. As an example, registry records at https://oixnet.org/identifier can present as 4 file types: HTML for human consumption and XDI, RDF and JSON for machine reasoning.

Also missing in the current identity infrastructure is the use of persistent identifiers. Prior to the web, individuals in the U.S. often used their Social Security Numbers (SSNs) as identifiers. Because SSNs were also tied to individual financial accounts, the knowledge of someone's SSN became a means of theft of their financial assets, especially with the rise of online financial transactions. Now we keep our SSNs secret, only sharing them with trusted entities.

New identifier(s) must step in to fill the void. As corporations, IdPs in the United States have two readily available public persistent identifiers that can be used in the OIXnet Registry:

- **Employer Identification Number** (**EIN**) is also known as a Federal Tax Identification Number, and is used to identify a business entity. U.S. employers must have an EIN, including businesses, nonprofit organizations, and state or local government agencies. This widespread use makes the EIN a handy reference number for finding information about organizations. An EIN for a publicly traded company must be listed on the first page of the Securities and Exchange Commission filing document, which is available to anyone online.

- **International Standard Name Identifier (ISNI)** [ISO 27729] ISNI is the International Standards Organization (ISO) certified global standard number for identifying entities including corporations. It is part of a family of international standard identifiers that includes identifiers of works, recordings, products and rights holders for established standards, e.g. DOI, ISAN, ISBN, ISRC, ISSN, ISTC, and ISWC. The mission of the ISNI is to assign to the public name of an entity a persistent unique identifying number in order to resolve the problem of name ambiguity in search and discovery; and to diffuse each assigned ISNI across all standards in the global supply chain so that every published work can be unambiguously attributed to its creator wherever that work is described.[1]

The Power of Linked Data

When data is linked, replication is reduced and accuracy increased. By using a persistent identifier, physical address information does not need to be duplicated. It can always originate from the persistent identifier and the entity only needs to make the update once. ISNIs, as Linked

[1] http://www.isni.org

Open Data identifiers, create a bridge between multiple domains (silos) and they are a critical component in machine reasoned applications.

Linked Data also enhances security by isolating data elements to their origins and making those data available at network scale. What is needed is a new network of human attributes which can transact at network scale. The Open Identity Exchange Network (OIXnet) is the start of that network, a new protocol for human attributes starting with IdPs and the provenance of their assertions.

Jump Start Digital Identity

The OIXnet Registry Pilot Project, using the **Design-Use-Build** (DUB) methodology, immediately constructs URIs for IdP's as Linked Open Data for machine reasoning and human consumption with the following data elements in HTML, XDI, RDF and JSON formats:

REQUIRED for Registry Record (public):

Persistent identifier - ISNI and EIN (when available)
Displayed ISNI in OIXnet Registry URL
Entity name must match persistent identifier name
Administrative contact (organizational role or person)
Technical contact (organizational role or person)
Protocols used
Protocol certifications
URI/URL where human attributes are retained (domain name)

OPTIONAL for Registry Record (public or restricted to registrants):

Attribute types (private, commercial, and/or public)
Attribute conditions, (opt-in, opt-out, no option)
Ontologies/schemas used
NIST LOA rating

This initial prototype registry will allow data structure modifications by pilot participants to occur quickly and it will provide trusted identity attributes to inform machine reasoners and human identity consumers. The registry begins with 256 bit encryption at https://oixnet.org/identifier as a URI/URL with documented machine provenance with the goal of National Institute of Standards and Technology (NIST) Level of Assurance LOA 3+ environmental conditions.

OIXnet Registrants can immediately make use of ISNIs for human researchers by use of Open Researcher and Contributor IDs (ORCID's), which are a subset of ISNI where the entity must be human. There are currently over 1 million registered ORCIDs worldwide for highly influential people in higher education and scientific research fields. Connecting persistent identifiers adds value to

ORCID owners and OIXnet Registrants by allowing the rapid aggregation of cross domain attributes from multiple IdPs. Commercial attributes are enhanced by more structured data.

New Digital Identity Potential

The OIXnet Registry will facilitate the ability to aggregate and disaggregate personal attributes of **condition**, **contribution** or **consumption** through a Trust Framework enabling rapid control and construction of persona in Cyberspace.

The fluid control of our attributes at velocity, without friction and latency, provides a new foundation for awareness in Cyberspace where we command assets and negotiate liabilities to our benefit. By extension, we become something more with new capacity.

Commercial opportunities increase with the availability of more personal data. When attributes are trusted, commercial services can be employed to improve our results. "Big Data" demonstrates just how predictable behaviors can be. When our behavior becomes part of a larger measure analyzed by reasoners, serendipity increases.

A researcher decides to share his ORCID (including his employment history and published works), his social network identities, his biometric information obtained by wearable devices, and his email address with machine reasoners. New commercial services which enhance the value of these data emerge as new mobile apps which inform him (with his consent) of new opportunities based on his current environment.

Using location data, a possible new mobile app could be created to notify researchers when they are in physical proximity to a person meeting certain conditions. For example, a researcher might ask to be notified when he is within 30 feet of someone who has attended 3 out of the last 5 biomedical conferences he has also attended, or is a stamp collector and has agreed to share personal data. The researcher then finds himself with 2 hours to kill in Malpensa Airport outside Milan when his phone displays the message, "There's a person within 30 feet who also attended conference X, Y and Z and also attended the same undergraduate university as you, 10 years later. Would you like me to let him know you are nearby and interested in conversation? I see that his plane does not leave for 3 hours." This is serendipity at its best. The commercial opportunities for individual trusted data are endless.

OIXnet Registry begins the formation of a new Internet protocol for human identity attributes to facilitate security, privacy and value in identity attribute exchange. What the World Wide Web did for information is what OIXnet can do for digitalized human attributes. The instability created by continued hacks on personal data reinforces the need for a new, secured lane on the Internet, where known entities can choose to interact to the benefit of individuals, and where personal assets are protected.