5 – The Personal Information Ownership Component

Hey! You! Get off of my cloud

The Rolling Stones

Question 5 *Personal control of information about oneself has been a long-sought goal of privacy activists. How can a universal identity credential restore privacy rather than erode it even further?*
Answer 5 The Personal Information Ownership Component
The foundation of real privacy is your own control over information that identifies you. Without such strong controls, individuals will rightfully resist the idea of a strong identity infrastructure. While the companies that accumulate information about you regard that information as their own corporate asset, the PIOC provides technological and legal tools by which you can reclaim that asset as your own personal property. The PIOC accomplishes accountable anonymity, letting you assert your identity without revealing your identity.

Michael Gartenberg Is Scary
Those who use iTunes to share files among multiple devices have a sense of the elegant convenience of having all your "stuff" available anywhere. iTunes is of course Apple's version of the personal cloud. If you don't think about who else is in that cloud and why they're so interested in being there, the ease and convenience of it all is practically hypnotic. Things are hypnotic when hypnotists want them to be.

To some, "personal cloud" means a Dropbox-type shared online personal storage facility. But the personal cloud will soon become much more than that.

Gartner research director Michael Gartenberg gives us a vivid picture of the encompassing nature of the personal cloud that's coming into existence in his video at http://www.youtube.com/watch?v=PFV2M2FIPo4&feature=plcp.

Do watch that video. Take in Gartenberg's glassy, almost hypnotized stare, the black-on-black visuals, and the tinkling elevator music in the background. Is that video not one of the scariest things you've ever seen? Doesn't he look like one of those automatons in the famous Apple "1984" commercial?

"Personal cloud, business cloud, government cloud, social cloud, and they all revolve around three things: synchronization, storage, and streaming. Taking my content, mov-

ing it online, accessing other peoples' content, and the ability to seamlessly share with others as they need it," he says, with complete acceptance.

Seamlessly share my content with others as they need it? Um, who exactly are "others" and if they think they need my content, do I get to decide whether they should have it?

By the way, "Yes" is the only answer I find acceptable.

"You must pay attention to the personal cloud because that is the focus of the consumer digital lifestyle." It's hard to disagree with that one. The personal cloud will be our new home, our second home, unless we go off the grid and live off the land somewhere in the Yukon. So shouldn't we give this personal cloud thing a little scrutiny, rather than glassy-eyed acceptance of a cardboard box domicile by the side of a busy street?

"Whoever controls synchronization to the personal cloud, well, they're going to control the world."

Whoa, slow down there Mike!

If things continue the way they're going, my guess is that Arpanet III will control synchronization to the personal cloud. After all, they're the only ones who don't have to worry about meeting the demands of the patchwork of privacy legislation around the world. They don't need to comply with anything other than the rules that govern honor among thieves.

But let's say that's just paranoid. Let's say a "legitimate" organization like Apple or Google or Microsoft or Google/DoubleClick ends up controlling synchronization, and therefore controlling the world. Excuse me for not breathing a sigh of relief. We all know what power does and we know what absolute power does. I would rather do this synchronization, storage, and streaming on my own terms, from my own place.

The Question, Well Posed:

John Sabo sums up[66] the aggregated problem of identity and privacy:

> If carried out close to its ultimate vision, the Identity Ecosystem will be composed of a huge, interlocked network of identity and attribute providers, relying parties, individual consumers and citizens, an unimaginable number of interdependent applications, services and devices, standards, and competing regulatory and audit requirements. In such an environment, is it possible to have any assurance of privacy? Are privacy risks understood and manageable?

The Answer: YES

Sorry if that sounds glib, but the answer is yes, we can understand and manage privacy risks. We just need to stop obsessing about how Internet folks are approaching the

66 Ian Glazer of Gartner, quoting John Sabo, Director, Global Government Relations for CA Technologies in a presentation entitled "An Introduction to the 3rd Epoch of IDtrust" at the 2012 NSTIC/IDtrust Workshop, "Technologies and Standards Enabling the Identity Ecosystem," March 13, 2012, at NIST in Gaithersburg, MD.

problem and look to the real experts. You'll find them among notaries public and the administrators in vital records departments. Teach them a little PKI, give them enrollment, certification, and privacy tools, and they'll have the problem solved for us, where "us" means "those of us who are willing to accept the jurisdiction of an online city hall in the same manner that we accept the jurisdiction of the physical city hall where we live."

In other words, this is not a solution for those who choose to live and work in cardboard boxes alongside the outdoor information highway. Sadly, homeless folks have very little assurance of privacy.

Hey Mike, Synchronize This!

Buildings provide people and organizations with the security needed for Quiet Enjoyment, a place where things can get done. Of course that's not all that buildings are good for. Quiet Enjoyment implies privacy as well.

There's a good chance you're reading this book sitting in a comfortable chair, in a room, in your home — in the privacy of your own space. Nobody is looking over your shoulder, taking notes on how you react to every page, or what socks you're wearing, or what you're drinking. Quiet Enjoyment is very much about securing your personal privacy.

We've noted that society has become conditioned to accept fraud and theft as normal business practices. Changing that calls for a means to preserve and respect your property rights, starting with some of your most important property, the information that identifies you. Because if information about you isn't your property, then whose property is it?

The goal of privacy activists has always been to give people control over the use of information about themselves. That's admirable. And supposedly it's difficult.

I don't think it's difficult at all.

Largely, it's a matter of starting with the right assumptions. Changing peoples' assumptions, now that can be difficult. But we at The Authenticity Institute are up to the challenge.

One of the assumptions that gets in the way of personal ownership of personal information is the notion that because a reliable identity is necessary to establish that it is in fact you who is claiming ownership of information about you, then that reliable identity credential will eliminate your ability to be anonymous. That's no longer true. Done right, reliable identity improves your ability to be anonymous.

A related old notion is that a reliable identity will erode privacy in general. And as long as you assume that someone else owns and controls your reliable identity, that can easily be true. But why would we assume such a thing?

We assume it because we've been led to believe that's the way it has to be. Marketers and government agencies and software vendors and healthcare providers and insurers and credit bureaus and social networks own your identity.

Well, that's just nonsense.

Establishment of reliable identity and disclosure of identity information are entirely different things.

If we're going to own the information about ourselves, we need a way of establishing that I am me and you are you, a reliable way of knowing that the person exerting control of his or her personal information is really the person identified. We need a reliable identity credential. Privacy requires reliable identities.

A system of identity reliability, done right, gives us a fortress of privacy.

On the other hand, a universal identity system done wrong is a big threat to our privacy. And in fact that's what we have now: a very bad system that provides marketers and government agencies and software vendors and healthcare providers and insurers and credit bureaus and social networks with enough data about you to track your every move, while providing you with nothing to prove that an impostor is not you – and nothing to tip you off that the eleven year old girl in an online social space with your daughter is really a 40 year old guy. They cynically advise you to protect your social security number or national ID number, and shred your bank statements, all the while knowing that these measures are useless in the age of online table joins and cookie clubs.

A good identity system does what your car registration is supposed to do: It provides accountability by letting anyone see your license plate number, while keeping your identity confidential unless someone has a legal right and need to know it.

The Personal Information Ownership Component empowers you to own information about yourself and to control its use.

The computer or phone or tablet or other information appliance of the future can serve us or it can continue to serve the factions of manufacturers and service providers behind it. The choice is up to us, the people who are willing to take the trouble to claim control over their property, that is, their information and their information appliances.

If we know what to ask for, we can ensure that our information infrastructure serves us in a viable manner. “Viable” means not requiring eternal vigilance, constant reading of linked privacy statements that many companies don’t actually even honor. The system must deliver technology that protects our information and have legal components that provide protections with teeth.

Your Personal Office and Your Personal Assistant

You'll recall that InDoor spaces are built with PKI construction materials, and carry occupancy permits signed by individual professionals who are individually liable for any deficiencies in their design and construction that lead to breaches of quiet enjoyment.

We've referred mostly to offices and meeting rooms and other social-type spaces in our discussion of InDoor spaces, but now let's introduce another type of InDoor space.

The user interfaces of social networks typically have a tab that's labeled “Home.” Click on it and you're brought to a “profile” of yourself, whatever that is.

A MyOwnHome by contrast looks and acts as much like a physical home as possible in two dimensional space. (A virtual reality, 3D version of MOH will be available for those who like VR environments.) It includes common spaces such as living rooms and dens.

But that's all user interface niceties. Let's get into what makes your MOH really special.

A MyOwnHome may be built inside any authenticity-enabled social network community, or Village®. As the owner of your MyOwnHome, you're in charge of its access controls and privileges, its exterior and interior design.

But the really special part of your MyOwnHome is its MyOwnOffices. You'll find one MyOwnOffice for each adult inhabitant.

All InDoor spaces are access-controlled, with access permissions set by — whom else? — the owner of the space. Your MyOwnOffice is a special kind of InDoor space in that in the default configuration, you are the only person allowed in. Built of the best PKI construction materials, it's a room that is absolutely under your control.

Actually there are two more "people" in the default version of your MyOwnOffice. One is your MyOwnAssistant is a software robot whose job is to respond to requests for information about you, strictly according to your wishes. You also can allow another individual, such as a spouse, access. Everyone else in the world stays outside.

To accommodate those outsiders, your MyOwnOffice has an exterior wall with a service window that works like the a bank drive up window, with the virtual version of one of those secure slide-out drawers that transfers cash and documents between you and the teller. Your MyOwnAssistant sits at that service window, responding to requests from supplicants who may pull in off the information highway and drive up to the window.

And what else is inside? This is where it gets really interesting. Inside your MyOwnOffice you'll find at least one file cabinet called MyOwnInformation. MOI.

Your MOI is your collection of information about you, organized so that you can manage the sharing of any particular piece of information. If you change a phone number, then all who are entitled to know it have access to it. If the reason for the change is to deny it to someone who previously had it, well, that's easily done.

We mentioned that the Personal Information Ownership Component provides not only a technology framework for protection of your private information but a legal framework as well. That legal framework is built with two construction materials: copyright law and secrecy law.

Copyright generally applies to "works" such as films, play scripts, images, music, and books, including reference works. And so we need a reference work about you.

Your Biographical Reference Work includes both narrative text and tabular data. Tabular data makes it possible for your MyOwnAssistant to control the disclosure of any chunk of information about you without disclosing other chunks that you might not want to disclose.

Your MyOwnInformation file cabinet also can include any other information you feel needs to be absolutely under your control. Additional MOIs in your office contain the Biographical Reference Work and other information on each of your dependents.

When a digitally signed request is presented at the service window, the first thing your MyOwnAssistant will do when is check for the digital signature of the visitor on your Personal Nondisclosure Agreement, and for license granted to give the visitor access to the information requested. If no signed PersonalNDA is on file for the party represented by the public key, your assistant will present your PersonalNDA form, and its Exhibit A, Application for License, which includes spaces for identifying which items of information are requested.

That dialog between your assistant and the requesting party (the "supplicant") can happen in either of two ways. If you're applying for a policy with an insurance company, it will take the form of a query dialog using the SAML protocol, with your PersonalNDA taking the form of an XML document, probably in a batched procedure, with no human being actually participating in the dialog.

To go into detail on that here would be to bury the legal essence of what is being done. Instead we will show the second case, probably the less common one, in which an individual requests pieces of information about you via a web page.

Here is what the individual requesting party (supplicant) will see:

Please sign my Personal Nondisclosure Agreement

You have requested certain information about me. Before I consider disclosing that information to you I will need to have you digitally sign this PersonalNDA using the PEN of an identity certificate that represents an identity quality score of at least 22.

Please review this document and then click on the button at the bottom of this page to sign it and send the signature to me. If your browser does not facilitate signing, you may download a .doc, .odt, or .pdf of the document that has been signed by me, and use your word processor to sign it with your PEN.

Please note that this creates no obligation on my part to disclose anything.

And the actual PersonalNDA form:

PERSONAL NONDISCLOSURE AGREEMENT
of the person represented by the identity known as
RC94873784

This Agreement is entered into this __th day of _____, 20__ by and between [name], an individual who is represented by the identity **RC94873784** (hereinafter referred to as "Owner"), and The City of Osmio (hereinafter referred to as "Supplicant").

Owner has established that all information that may be used to identify himself (hereinafter referred to as Personally Identifiable Information or PII) is to be considered Proprietary and Confidential, specifically proprietary to Owner and Confidential and to be disclosed only under license. Such Personally Identifiable Information includes

1. Name given on birth certificate
2. Current name
3. Diminutives, nicknames, and aliases
4. Associations, linkages, or bindings of any of the names above with any usernames or Identity Commons assertable identities such as OpenID, i-Card, i-Name, Shibboleth Name, etc.
5. Associations, linkages, or bindings of any of the names above with any electronic mail addresses or any telephone number
6. Associations, linkages, or bindings of any of the names above with any employer, membership organization, school, healthcare provider, insurer, bank, or other financial institution
7. Associations, linkages, or bindings of any of the names above with any Physical Addresses including legal address of residence and all former addresses
8. Associations, linkages, or bindings of any of the names above with any personal biographical information including history, names of family members, names of schools attended, names of current or former employers, associations with any organization, real or personal property, vehicles and their registration numbers, or any other information that could in any way be used to develop an association between the names above and any entity.

Owner is hereby willing to disclose Personally Identifiable Information to Supplicant in connection with both parties' entering into a business relationship or other relationship and only under the following conditions:

1. All Personally Identifiable Information disclosed shall fall within the terms of this Agreement.
2. Supplicant agrees to take all reasonable precautions to safeguard Personally Identifiable Information disclosed to them by Owner and to hold in confidence for a period of fifty (50) years all such Personally Identifiable Information.
3. It is necessary and desirable that certain Personally Identifiable Information be disclosed to Supplicant and that employees of Supplicant have contact with Owner. Supplicant acknowledges that the disclosure of Personally Identifiable Information, as defined in this Agreement, and the obligations herein are good consideration for Supplicant fulfilling its obligations under this Agreement, and that any Personally Identifiable Information that Owner discloses to Supplicant will be received and maintained by the Supplicant in trust and confidence.

Supplicant will take all necessary action to ensure that there is no unauthorized disclosure of Personally Identifiable Information by it or any of its employees or persons with whom it deals; and if it becomes necessary and proper for Supplicant to disclose proprietary information to any of its employees or persons with whom it deals, to hold such Personally Identifiable Information in trust and confidence subject to the restrictions in this Agreement.

Except as directly necessary for the performance of dealings between the parties, Supplicant will not reproduce, use, or disclose to others any Personally Identifiable Information without the prior written consent of Owner.

4. All Personally Identifiable Information of Owner will remain its own property, regardless of its disclosure to Supplicant. This information is a valuable personal asset and the protection of such information is therefore essential. Within thirty (30) days following a request or the completion of business dealings between the parties, Supplicant will return any and all copies of such Personally Identifiable Information; in which case Supplicant will destroy them and within such thirty (30) day period certify in writing their destruction.
5. It is understood by both parties hereto that this Agreement does not constitute a license to use the Personally Identifiable Information. Such license, if issued, will be provided as Exhibit A to this agreement, or will be provided separately.

Owner and Supplicant agree that this Agreement and all disputes arising hereunder are governed by the laws and courts of the Republic and Canton of Geneva and that breach of this Agreement will cause irreparable harm to Owner. Both parties agree that in the event of breach of this Agreement, the injured party shall be entitled to equitable relief in addition to any other remedies it may have in order to restrain such breach. Equitable relief will include, but not be limited to, penalties for unauthorized disclosure of Personally Identifiable Information as specified by the Graham-Leach-Bliley Act of the United States of America. If Supplicant breaches or threatens to breach any of the Non-Disclosure covenants herein, Owner, in addition to any other remedies it may have at law or in equity, will be entitled to a restraining order, injunction, or similar remedy so as to specifically enforce such provisions. The parties acknowledge that money damages alone would be an inadequate remedy for injury that would be suffered by a breach of any of the provisions of this Agreement.

This Agreement constitutes the entire agreement between the parties hereto and its terms may not be modified, altered, or cancelled except by further written agreement signed by Owner or an authorized officer of Supplicant or, if Supplicant is an individual, by Supplicant.

By their digital signatures accompanying this Agreement, the parties hereto have indicated below their acceptance of this Agreement as of the date [capture date].

OWNER SUPPLICANT

[to be digitally signed with Owner's PEN or other signing key] [to be digitally signed with Supplicant's PEN or other acceptable signing key]

[date stamped] [date stamped]

EXHIBIT A to PERSONAL NONDISCLOSURE AGREEMENT

APPLICATION FOR LICENSE

You have requested the following information about me: MY NAME

If you would like to request additional items of information about me, please enter them here:

- First additional item:
- Second additional item:
- Third additional item:

If you agree to the disclosure of the information identified in Exhibit A, the License Application, then you can proceed and issue the License:

LICENSE

_____, hereafter referred to as LICENSEE, is hereby granted the license to have access to the following information (Licensed Information) about the person identified herein as RC94873784:

Name
Gender

Licensed Information, as updated from time to time, may be retrieved at any time during the term of this license by accessing the Owner's MyOwnOffice using Licensee's Reliable Identity Credential.

Permitted use of Personally Identifiable Information as identified in the Personal Nondisclosure Agreement of which this Exhibit A is part is as follows: The information disclosed under this license is for use of LICENSEE only, and only for the purpose of

First purpose:

Additional purpose:

Additional purpose:

and is not to be shared with any other party without an additional license from the person identified herein as RC94873784 to do so.

If a PersonalNDA signed by the supplicant already exists but you have not issued a license that covers the specific information requested, your assistant will ask the supplicant (that is, the relying party) to fill in and sign a new PersonalNDA with the additional items.

If this all sounds cumbersome, consider that your assistant and the supplicant will normally be pieces of software that talk to each other via an API. The information exchanged is in an XML-based personal information markup language. Once you have filled in your Disclosure Practice Statement form telling your personal assistant exactly which groups and individuals are entitled to see which items of information, you needn't be bothered at all until someone asks for something that you have not authorized via your Disclosure Practice Statement.

You may write your own PersonalNDA, but that introduces a big inefficiency. If you use the standard PersonalNDA, the relying party can robo-sign it, in an automated process, probably in a batch with thousands of others. By using the standard PersonalNDA language you enable the relying party's API program to know (perhaps confirmed by either diffing or hashing the non-variable parts) what it is signing without actually requiring a human being to read it. A custom PersonalNDA will be unworkable for most relying parties.

You will have the benefit of a recommended set of licenses to issue to credit bureaus, insurance companies with whom you have a relationship, government agencies, etc. You'll also have recommended licenses for close and extended family, friends, professional colleagues, etc.

Your assistant can operate in either browser mode or server mode. Your insurance company, for example, having previously signed your PersonalNDA and obtained a license from you, would use server mode to retrieve your updated address. For that matter, all such administrivial relationships will be taken care of automatically without bothering you.

Think about it. Never again have to fill in a form with personal information. A supplicant operating in server mode might send out a million requests at once, with the supplicant's signing officer signing thousands of PersonalNDAs at a time, in batch mode.

Identity Management via MyOwnInformation

The cloud computing revolution has raised major concerns in federated identity and federated identity management. A multitude of companies are scrambling to get their piece of the market for…what exactly? Managing identities created through…what?

The only way cloud identity management will work is if the identity record is under the control of the subject of the identity, and attested to by public authority.

A number of cloud identity-management protocols have served up the usual steam-

ing hot bowl of acronymic alphabet soup: SCIM, SPML, DSML, each of which is accompanied by a dozen brand names of vendors who would like you to think of it as their invention at the same time hoping you appreciate how standards-compliant it is.

Each cloud identity management system consists of an XML data type definition, and any could serve as a meager starting point for a robust personal information store, called MyOwnInformation (MOI) inside the subject's MyOwnOffice. It's meager because it's an organizational information store. Imagine collecting all the information about yourself in file cabinets and in your phones and piece in a data field inside an XML document, to be absolutely locked up but to be made accessible in pieces only under license to signers of your PersonalNDA. The DTD will be longer than this book.

But for now we need to choose a format.

Let's choose SCIM.

Here is the "non-normative example of the fully populated SCIM representation in JSON format" from the System for Cross-Domain Identity Management: Core Schema 1.1[67] (SCIM version 2), originally known as Simple Cloud Identity Management (SCIM).

```
{
 "schemas": ["urn:scim:schemas:core:1.0"],
 "id": "2819c223-7f76-453a-919d-413861904646",
 "externalId": "701984",
 "userName": "bjensen@example.com",
 "name": {
 "formatted": "Ms. Barbara J Jensen III",
 "familyName": "Jensen",
 "givenName": "Barbara",
 "middleName": "Jane",
 "honorificPrefix": "Ms.",
 "honorificSuffix": "III"
 },
 "displayName": "Babs Jensen",
 "nickName": "Babs",
 "profileUrl": "https://login.example.com/bjensen",
 "emails": [
 {
  "value": "bjensen@example.com",
  "type": "work",
  "primary": true
 },
 {
  "value": "babs@jensen.org",
```

67 http://www.simplecloud.info/.

```
     "type": "home"
    }
    ],
    "addresses": [
    {
     "type": "work",
     "streetAddress": "100 Universal City Plaza",
     "locality": "Hollywood",
     "region": "CA",
     "postalCode": "91608",
     "country": "USA",
     "formatted": "100 Universal City Plaza\nHollywood, CA 91608
USA",
     "primary": true
    },
    {
     "type": "home",
     "streetAddress": "456 Hollywood Blvd",
     "locality": "Hollywood",
     "region": "CA",
     "postalCode": "91608",
     "country": "USA",
     "formatted": "456 Hollywood Blvd\nHollywood, CA 91608 USA"
    }
    ],
    "phoneNumbers": [
    {
     "value": "555-555-5555",
     "type": "work"
    },
    {
     "value": "555-555-4444",
     "type": "mobile"
    }
    ],
    "ims": [
    {
     "value": "someaimhandle",
     "type": "aim"
    }
```

```
    ],
    "photos": [
    {
             "value":     "https://photos.example.com/profilepho-
to/72930000000Ccne/F",
     "type": "photo"
    },
    {
             "value":     "https://photos.example.com/profilepho-
to/72930000000Ccne/T",
     "type": "thumbnail"
    }
    ],
    "userType": "Employee",
    "title": "Tour Guide",
    "preferredLanguage":"en_US",
    "locale": "en_US",
    "timezone": "America/Los_Angeles",
    "active":true,
    "password":"t1meMa$heen",
    "groups": [
    {
     "display": "Tour Guides",
     "value": "00300000005N2Y6AA"
    },
    {
     "display": "Employees",
     "value": "00300000005N34H78"
    },
    {
     "display": "US Employees",
     "value": "00300000005N98YT1"
    }
    ],
    "x509Certificates": [
    {
     "value": "MIIDQzCCAqygAwIBAgICEAAwDQYJKoZIhvcNAQEFBQAwTjEL-
MAkGA1UEBEzAhMCVVMxRBgNVBAgMCkNhbGlmb3JuaWExFDASBgNVBAoMC2V4Y-
W1wbGUuY29tMRQwEgYDVQQDDAtleGFtcGxlLmNvbTAeFw0xMTEwMjIwNjI0Mz-
FaFw0xMjEwMDQwNjI0MzFaMH8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWx-
```

pZm9ybmlhMRQwEgYDVQQKDAtleGFtcGxlLmNvbTEhMB8GA1UEAwwYTXMuIEJh-
cmJhcmEgSiBKZW5zZW4gSUlJMSIwIAYJKoZIhvcNAQkBFhNiamVuc2VuQGV4Y-
W1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7Kr+D-
cds/JQ5GwejJFcBIP682X3xpjis56AK02bc1FLgzdLI8auoR+cC9/
Vrh5t66HkQIOdA4unHh0AaZ4xL5PhVbXIPMB5vAPKpzz5iPSi8xO8SL7I7SDhcBVJhqVqr3Hgl-
lEG6UClDdHO7nkLuwXq8HcISKkbT5WFTVfFZzidPl8HZ7DhXkZIRtJwBweq4b-
vm3hM1Os7UQH05ZS6cVDgweKNwdLLrT51ikSQG3DYrl+ft781UQRIqxgwqCfX-
EuDiinPh0kkvIi5jivVu1Z9QiwlYEdRbLJ4zJQBmDrSGTMYn4lRc2HgHO4DqB/
bnMVorHB0CC6AV1QoFK4GPe1LwIDAQABo3sweTAJBgNVHRMEAjAAMCwGCW-
CGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgN-
VHQ4EFgQU8pD0U0vsZIsaA16lL8En8bx0F/gwHwYDVR0jBBgwFoAUdGeKit-
caF7gnzsNwDx708kqaVt0wDQYJKoZIhvcNAQEFBQADgYEAA81SsFnOdYJtNg5Tcq+/
ByEDrBgnusx0jloUhByPMEVkoMZ3J7j1ZgI8rAbOkNngX8+pKfTiDz-
1RC4+dx8oU6Za+4NJXUjlL5CvV6BEYb1+QAEJwitTVvxB/A67g42/vzgA-
toRUeDov1
      +GFiBZ+GNF/cAYKcMtGcrs2i97ZkJMo="
    }
    ],
    "meta": {
    "created": "2010-01-23T04:56:22Z",
    "lastModified": "2011-05-13T04:42:34Z",
    "version": "W\/\"a330bc54f0671c9\"",
      "location": "https://example.com/v1/Users/2819c223-7f76-
453a-919d-413861904646"
    }
  }

Thousands of data elements need to be added to this to make it a functioning MOI — enough to keep Osmio's Privacy Board busy for a long while. If you have a talent for XML-type data representations, consider presenting your credentials for Board membership. Among other things the Board's job is to produce and maintain a Personal Information Markup Language (PIML) based upon SCIM.

C2B

Since the Web began, sites and initiatives and organizations have been relentlessly categorized as either B2B or B2C, business-to-business or business-to-consumer. Business initiates at us; we sit and let business have at us.

Something's missing.

What we need are expressions that start with C rather than B, a little C2B where consumers write the rules, and the business follows them.

No, really. Forget your "you're very important to us, please listen to some elevator music on hold while we wait for you to go away..." And spare us your insipid and insulting ad copy telling a million people all at once that "you're special, you're an individual."

Here are my rules: Sign my PersonalNDA or go away.

If a supplicant is a member of a group that is defined by you or by the recommended licenses list, they will have access to specific items of information if they have signed your PersonalNDA, and you have granted them a license which specifies exactly what information they may have access to, for what purposes, for how long, and which also specifies that they may not share that information with any other party without your prior digitally signed permission.

The license specifies that they will honor the penalty recommended by the U.S. Federal Trade Commission for breaches of the personal privacy provisions of the Graham-Leach-Bliley Act, regardless of whether they are in the United States. And it specifies that an identical damages payment will be paid to you personally in addition to the fine paid to the government.

That recommended penalty is $11,000 per instance. That's $11,000 to the government and $11,000 to you.

So go ahead Google DoubleClick, go ahead Facebook, share that information asset of mine. Make my day. Eleven grand may not be much to Google, but it'll make for a nice family vacation for me...

And music industry, you set the right tone by holding people accountable for their illegal file sharing. So here it is right back atcha. Pay me eleven grand for that information about my music preferences that you stole. And no, you may not pay the damages in the form of download credits. Cash please.

The Seed of the Authenticity Economy

You may be asking, "Will Google and Facebook and credit bureaus and page-view-tracking services and insurance companies sign these PersonalNDAs?"

The answer is: of course not. Thousands of larcenous commercial enterprises, governments, and noncommercial organizations have gotten used to regarding your personal information as their own balance sheet asset. We are advocating that people simply step in and remove that stolen asset and put it right back where it belongs: inside the home offices of the people identified.

They will detest the whole idea. They'll try to ignore it, and work hard to discredit it.

While they're busy trying to marginalize the idea of personal ownership of one's own personal information, the Personal Information Ownership Component and the Quiet Enjoyment Infrastructure of which it is part will provide an opportunity for startups in search, social networking, insurance, banking, etc. to serve a small but growing set of communities whose members value their personal information assets.

That is the Seed of the Authenticity Economy

The Authenticity Economy will be the source of new jobs as well as new business opportunities. The world simply needs a steady supply of authenticity, millions of metric tons of it. The asset required to transform a notary commission into a well-paid Attestation Officer profession is not money, but a track record of personal integrity. Unlike money, that's not something you can get tomorrow by selling your soul today.

Other licensed professions that will be brand new with the Authenticity Economy will be those of Architect, Contractor, and Building Inspector. All four will be involved in the creation of InDoor information infrastructures, that is, buildings.

Ownership of Information about You

We have described the architectural components of your Personal Information Ownership Component: your MyOwnHome, your MyOwnOffice, and file cabinets called MyOwnInformation for you and your dependents.

Inside your MyOwnInformation file cabinet is your Biographical Reference Work, your PersonalNDA form, your Disclosure Practice Statement, and the various Licenses you have issued to relying parties.

But your Personal Information Ownership Component is also a legal structure. We mentioned the PersonalNDA and license; now let's show how we establish your information as intellectual property, owned by you.

Intellectual property takes a number of forms, but for our purposes the important ones are copyright and trade secret.

How do you own information about you?

If the information is subject to copyright, the answer is simple: the copyright owner has title to the work. Often the rights to use the work are conveyed to others, but the copyright owner still owns it.

Now, who owns your name and address and the names of your children and your email address and other information about you? Copyright generally applies to "works," that is, books or music, not short snippets of information. So the answer is simply to assemble the snippets into a work. You can copyright a compilation of facts.

So, inside the virtual file cabinet called MyOwnInformation (MOI) is a "work," your Biographical Reference Work, a compilation of information all about you.

Your Biographical Reference Work

Here's what the U.S. Copyright Office has to say about its product:

WHAT IS COPYRIGHT?

Copyright is a form of protection provided by the laws of the United States (title 17, U.S. Code) to the authors of "original works of authorship," including literary, dramatic,

musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works. Section 106 of the 1976 Copyright Act generally gives the owner of copyright the exclusive right to do and to authorize others to do the following:

To reproduce the work in copies or phonorecords;

To prepare derivative works based upon the work;

To distribute copies or phonorecords of the work to the public by sale or other transfer of ownership, or by rental, lease, or lending;

It is illegal for anyone to violate any of the rights provided by the copyright law to the owner of copyright. These rights, however, are not unlimited in scope. Sections 107 through 121 of the 1976 Copyright Act establish limitations on these rights. In some cases, these limitations are specified exemptions from copyright liability. One major limitation is the doctrine of "fair use," which is given a statutory basis in section 107 of the 1976 Copyright Act. In other instances, the limitation takes the form of a "compulsory license" under which certain limited uses of copyrighted works are permitted upon payment of specified royalties and compliance with statutory conditions. For further information about the limitations of any of these rights, consult the copyright law or write to the Copyright Office.

WHO CAN CLAIM COPYRIGHT

Copyright protection subsists from the time the work is created in fixed form. The copyright in the work of authorship immediately becomes the property of the author who created the work. Only the author or those deriving their rights through the author can rightfully claim copyright.

In the case of works made for hire, the employer and not the employee is considered

Copyright law in other nations that are members of the Universal Copyright Convention is similar.

Beyond Copyright

Your Biographical Reference Work includes a copyright notice, and also carries the words:

"PROPRIETARY and CONFIDENTIAL. This information or any portion of it is only to be disclosed to Licensee, and is to be used by Licensee only in accordance with the terms of their License."

That's one step toward placing your Biographical Reference Work under the protection of secrecy law. The next piece of your PIOC that we'll establish to accompany it is your Personal Nondisclosure Agreement. Anyone who wants to have access to any of your information must digitally sign a copy of your PersonalNDA.

Each signed copy of your PersonalNDA is accompanied by a License for Use of Personal Information, which specifies exactly which items from your Biographical Reference Work are to be disclosed to the relying party, and how they may use that information, under penalty of the fine and damages described earlier.

In most cases the owner of a claimed copyright submits two copies of the work to the Library of Congress. Failure to submit copies, however, does not affect the copyright claim.

If you would like to deposit copies of your Biographical Reference Work with your country's copyright office, the forms are available at www.copyright.gov/forms for U.S. residents (with a submission fee of $30); at http://strategis.ic.gc.ca/sc_mrksv/cipo/cp/cr-appl-eng-2002.pdf for residents of Canada, and at www.hmso.gov.uk/copyright/guidance/guidance_notes.htm for U.K. residents. If you live in a non-common-law country your access to the benefits of PIOC may be more complicated.

Thwart the Cookie Clubs

Your Personal Information Ownership Component gives you legal ownership of your Personally Identifiable Information, your PII. You determine who gets to see what.

If the cookie clubs operate anonymously and outside the law, you might ask, how is a legal technicality like information ownership going to affect their activity? The cookie clubs, like the Mafia, have no legal existence, present no legal entity to sue or person to hold accountable. But the raw material they use is borrowed from legitimate corporate databases, and the methods used to collect it are subject to the concerns of management who worry about the company's name and brand.

Collecting a little bit of information illegally is not that difficult, but collecting information about millions of people illegally is very difficult because it becomes so visible. By taking legal possession of your PII and licensing it, you join a system that makes it impossible. The system relegates information theft back to a small, marginal cottage industry.

Claims of personal control over personal information have been made many times, only to turn out to have some very significant fine print. With Hailstorm/.NET My Services, for instance, you don't directly manage your own information; you appoint a partner who has free run of all of your information.

We have noted that the key to taking control away from those who would use your PII to control you is to take ownership of it. Now let's describe how you implement that ownership and control.

The Personal Information Ownership Component specifies communication between supplicant and information owner using Agent Communication Language (ACL) and Knowledge Query Manipulation Language (KQML), two established protocols.

The file resides in your MyOwnInformation file cabinet, which in turn is found in your MyOwnOffice. As with any online office, it can physically be served from any facility that meets building code and carries an occupancy permit. You can serve it from your cable-modem-connected personal computer, from a server in a large commercial hosting facility, or even on your PDA if you want to prove a point.

Creating a separate license for every individual and every organization you deal with could get tedious. To simplify, you can create group licenses, or even copy them from a library of recommended licenses. Each is appropriate to a group defined by you or copied from a library of suggested groups, for example:

Close family
Extended family
Credit bureaus
Credit information aggregators (e.g., Equifax)
Banks in which you have a consumer account
Banks from which you are seeking personal credit
Banks in which you have a business account
Other banks
Vendors in general
Vendors in categories 1, 2, 3, etc.

Items of information referenced in a license would include things like:

Credit history
Employment history
References 1, 2, 3, etc.
Resume
Identities of persons in group 1, 2, 3, etc.

The license will automatically apply to any entity you declare to be a member of the licensed group, until you remove them.

If you are really confident that people will say only good things about you, you may put that confidence on display by enabling the signing of references by means of an AccountableAnonymity credential (see RentalCredential).

A category may be used to identify vendors with whom you maintain a close customer relationship, or vendors who specialize in your avocation, or vendors who sell something that you happen to need at a particular moment. If your car needs tires you will probably want to announce that fact along with the year, make, and model of your car to the limited set of entities identified as sellers of tires. You may simply choose the default list of tire dealers in your area, or edit the list. After you buy your tires, you'll put the tire merchants back into the "general vendors" category.

For most applications within a facility there will be no need to disclose any information whatsoever on a one-time basis. The Identity Reliability Component provides a true single sign-on credential that should be good for any application. If Alice has been granted certain access privileges in a commercial QEI-based office facility, and your secure Foundational Certificate attests either directly or through an intermediary certificate to the fact that you are indeed Alice, then there is no need for anyone to consult your PIOC.

The promise of user control over personal information has been made many times before, from P3P to Microsoft's Passport and HailStorm, to the issuers of countless privacy statements. Generally there is no way to track what happens to information about you, and little legal recourse if you feel that information has been abused.

Your Personal Information Ownership Component, by contrast, gives you a large measure of control over your information, by the following methods:

1. Anyone requesting personal information from you must digitally sign your PersonalNDA and the associated license with the private key of an identity with an IDQA score that equals or exceeds your minimum requirement.
2. The license takes the form of a signed query specifying particular items of information. If the license is subsequently altered by the relying party, your signature on the license will not verify.
3. If the license grants permission to an organization, only an individual with a digitally signed statement of a relationship with that organization will be allowed to query the information in your Biographical Reference Work. For example, if the individual is acting on behalf of a mortgage company and the license is issued to members of a group named "prospective lenders," then they can proceed with the query; otherwise they cannot.
4. All queries are documented, time stamped, and digitally signed by the individual making the query. The individual accepts the terms of the license to your information, which means that it can only be used for the specific purposes mentioned in the license.
5. If your license does not permit disclosure of all of the items requested by the person making the query, that person must either ask you to release the additional information or be satisfied with what he or she has.
6. The individual signer of your PersonalNDA and license is legally responsible for any misuse of your information. His or her employer may provide indemnity for such consequences, but as in all of the Quiet Enjoyment Infrastructure, everything is ultimately signed by individuals.
7. You may define as many groups and individuals in your group licenses as you like. You may add or delete pre-defined groups such as "credit bureaus" and "tire merchants," or create your own groups, at any time. You may exclude specific members of groups.

Beyond Access Control: Privilege Controls

Having control over the use of personal information has the same kinds of manageability benefits as the other ways in which increased control over information and communication adds to the manageability of corporate networks.

With PIOC, we can designate not only the rights of remote institutions but also those of the people closest to us. For example, we might have a new signed email message format for sending information directly to a person's schedule. When the message arrives, our scheduling program recognizes that it is a schedule supplication and consults the license. The license notes which of the following permissions applies to the sender:

1. Unrecognized party: auto-reply with polite who-are-you message
2. Recognized party with no scheduling privilege: auto-reply with I-will-take-a-look-at-it message
3. Recognized party that I never want to give the time of day to and I want him to know it: auto-reply with blunt decline
4. Recognized party that I never want to give the time of day to but I don't want him to know it: auto-reply with I-will-take-a-look-at-it message
5. Team member: allow them to reserve up to 30 minutes in my schedule subject to my confirmation, but not to see the schedule itself
6. Partners: allow them to set schedule but not displace other appointments in doing so, and to view my work schedule but not my personal schedule.
7. Assistants who manage my schedule: allow them to see and do whatever they need
8. Spouse: allow to see entire schedule, reserve only personal time
9. Events planner for civic group: allow to query my schedule for yes/no response only when searching for optimum time to schedule an event, or to enter a reservation request

Your to-do list can be managed the same way. Your spouse might have full privileges with your personal to-do list while others may only make requested entries.

It turns out that identity is as important to privacy and manageability as it is to security. If you have a means of knowing the identity of those who want information about you, then you can manage the disclosure of that information. Eventually a mature, widely deployed Personal Information Ownership Component allows us to eliminate every single bit of bureaucratic activity from our lives, to never fill in another form, never spend a whole day scrounging for input for our tax returns, never look at another piece of health-care paperwork. If you have to visit a hospital emergency room in a strange city, just hold your watch up to the reader, press your finger to it, enter your PIN, and start telling the nurse what ails you. Ditto airports, government buildings, banks.

Deploying PIOC

Taking ownership of your information also will make doing business with you easier and more efficient, and quite likely more profitable. Someday our computers and DVRs will have PIOC consent procedures built into their operating systems[68]. If someone wants to use your property they must first ask. Seems fair enough doesn't it?

But we don't have to wait for new technology to start putting PIOC to work. Just as the main components of the public licenses that govern the use of open source software are legal clauses and declarations, the same is true of the Personal Information Ownership Component.

There are two parts to implementation of PIOC before your available technology supports it. First is the copyright and secret protection that you create by establishing, executing, and conveying the proper documents to the proper parties. At some point that will be facilitated by the website that provides access to all of the QEI procedures.

The second is to start requesting a PIOC paragraph in privacy policies. Here's an example of how such a paragraph should appear in the context of other parts of a typical privacy policy:

Privacy Policy

Commitment to privacy and security

[use of name, email address, other personal information]

Statistical information

[How your information might be used after aggregation with personal information from others]

Links to other sites

[Disclaimer of responsibility for use of personal information by sites which this one might link to]

Security

[How personal information is protected on servers]

Contact

[Where to address questions and concerns]

PIOC Protection

68 If your information appliance uses an operating system that knows the difference between indoors and outdoors, such as the Dorren™ operating system, your PIOC is built in.

> If you have taken steps to place your personal information in a Personal Information Ownership Component that conforms to the PIOC Standard, we acknowledge that the information you have provided is your intellectual property, that it is protected by your copyright in the information, and that it consists of Secrets as defined by any applicable trade secrets case law or statutes. Furthermore we acknowledge that such information has been disclosed to us under the terms of the "shrink-wrap nondisclosure agreement" in your Personal Information Ownership Component, provided that the terms of said agreement conform to the PIOC standard. Therefore any willful disclosure by us of such information in any manner that violates the instructions in the "shrink-wrap nondisclosure agreement" in your Personal Information Ownership Component in place at the time such information was obtained may be considered infringement.

While this first phase of implementation of PIOC offers the benefit of immediate deployment with no new technology, it does not simplify the user's life but rather adds another item to the "eternal vigilance" list. Only when PIOC is ubiquitously supported in our information appliances and servers will it contribute unequivocally to Quiet Enjoyment.

So let's look at a little of the technology that has been developed for applying an individual's privacy instructions (DPS) to the operation of the information infrastructure.

Covering Your Fingersteps: Part One

So far we've shown how your PersonalNDA and license, Biographical Reference Work, MyOwnOffice, and MyOwnInformation file cabinet protect record-oriented information about you.

But that still leaves a problem. There's another source of detailed information about you, which has nothing to do with the record-oriented information we've just discussed.

Any system of identity credentials introduces the concern of trackability, and the more reliable the bigger the concern, unless specific steps are taken to make it difficult for governments and marketers and other nosy organizations to know where you've been online.

Done wrong, a universal identity credential gives Big Brother a tool by which to track your every move. That concern of privacy activists is well placed. Would you want a global village where everyone knows everyone else's business? Where a personal identifier made it possible for snoops and governments and cookie clubs to watch your every move, building tables of data about all your actions, including the web pages you look at and the people you hang out with and the things you buy?

Accountability in a village of 700 people may cost a certain amount of your privacy, but that kind of accountability without a well-engineered system of privacy protection in a global village of seven billion people would be a Kafkaesque nightmare.

In fact that nightmare is well on its way, and with it we don't even get accountability. All we get is loss of privacy.

Privacy has been thoroughly eroded by both "legitimate" business and by a new global online mafia. And so we have another source of information about you that must be protected. We must eliminate the means by which nosy secretive organizations know all about you without even needing to know your name or social security number or other national ID number.

Donna's Adventure in Anonymity

The Personal Information Ownership Component portion of The Authenticity Infrastructure provides two methods for keeping a universal identity credential from being tracked.

To explain, let's be inspired by Donna Doer. Donna is the CEO of a rapidly growing company in an exciting field. She's the kind of person that journalists love to write about and analysts love to follow around.

Now it happens that Donna's company is about to buy Albert Ailey's company. For the deal to go smoothly, the two need to meet to discuss Albert's role in the merged company. If word of such a meeting got out to analysts and journalists and investors, Donna or Albert might be accused of deliberately leaking the news to their friends, and that could mean big trouble. So as a matter of diligence, not deception, Donna and Albert need to cover their tracks.

Donna chooses an obscure restaurant in an undistinguished part of town for the meeting. And since everyone in town knows Donna's bright red Ferrari, she rents a gray Chevy Malibu from Ready Rentals. The smokescreen seems to work. But one sharp-eyed reporter sees someone who looks like Donna driving that Malibu out of the Ready Rentals lot, and asks the Ready Rentals manager if it was her.

Of course the Ready Rentals response is, “That's confidential information”

If on the other hand an investigator from the SEC presented a court order requesting that same information, Ready Rentals would disclose it, because that also is their legal obligation.

So Donna and Albert's lunch meeting is productive, they agree on a role for Albert in the merged company, and the news is released properly, so that all potential investors learn of it at the same time, preventing suspicions of insider-influenced trades.

The Rental Credential

Now let's apply that lesson to the Information Highway.

The Rental Credential is part of Personal Information Ownership Component. A particular Rental Credential is bound to your underlying Foundational Identity Certificate for a short period of time. The record of which rental credential went with which Foundational Certificate at which time is encrypted with a key that is controlled by the Chief Privacy Officer of the City of Osmio.

That information is to be decrypted and disclosed only at the direction of a License or court order from a "court of competent jurisdiction."

If you use a Rental Credential to establish basic accountability with a relying party, the relying party will likely want to know more than "this public key represents for a short period of time a living human being of undisclosed name, age, gender, domicile, etc." If it turns out that you would like to enter into a more significant relationship with the relying party, simply direct the relying party to your PersonalNDA form and License Application.

Or just forget the whole thing. Either way, you prevent others from establishing a shareable trail of bread crumbs showing where you have been, what you have done, what your interests and perceptions are, and how those perceptions might be manipulated.

Second Method: The ZK Credential

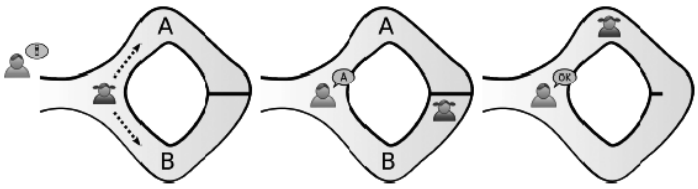
Our second method of providing accountable anonymity is based upon something called a zero-knowledge proof of identity.

It can be demonstrated that proving that you are who you say you are without revealing who you are is a subset of the problem of proving that you know something without revealing what you know.

How do you prove such a thing?

This little story[69] by Jean-Jacques Quisquater of the University of Louvain shows how that can be done without delving into the mathematics of complexity theory.

Peggy is a spelunker who claims to know a secret word that will open a magic door at the far end of a donut-shaped cave. You can only go all the way around the donut if you can open the door, as you can see below.



Peggy comes up with a solution. She labels the sides of the cave "A" and "B" and tells Victor to wait outside the cave for five minutes while she goes around to the door. After five minutes Victor is to shout the identity of the path, A or B, by which she is to return.

Victor shouts "A!" and Peggy returns by the A path, meaning that either she was lucky that Victor chose the side she was already on, or that she knows the secret.

They repeat the process dozens of times, with Peggy returning via the designated

69 "Zero Knowledge Interactive Proof," by Jean-Jacques Quisquater, http://www.dice.ucl.ac.be/crypto/publications/1990/alibaba.pdf; illustration by Dake.

path every time. Victor is convinced and offers the money. Peggy takes the money and says, “I'll tell you the secret over lunch, after you pay the tab.”

Some ZK Technology

We have mentioned the World Wide Web Consortium’s (W3C) Platform for Privacy Preferences (P3P). Shortly after P3P was developed, IBM’s Zurich Research Laboratory developed a set of more finely-grained protocols and a language, Enterprise Privacy Authorization Language (EPAL), with which to express privacy directions within the enterprise. According to its authors[70], EPAL is “a formal language to specify fine-grained enterprise privacy policies. It concentrates on the core privacy authorization while abstracting from all deployment details such as data model or user-authentication."

Its goal is to "develop a[n] interoperability language for the representation of data handling policies and practices within and between privacy-enabled enterprise tools, which serve to (1) enable organizations to be demonstrably compliant with their stated policies; (2) reduce overhead and the cost of configuring and enforcing data handling policies; and (3) leverage existing standards and technologies. EPAL should provide the ability to encode an enterprise's privacy-related data-handling policies and practices and [constitute] a language that can be imported and enforced by privacy-enforcement systems. An EPAL policy defines lists of hierarchies of data-categories, data-users, and purposes, and sets of (privacy) actions, obligations, and conditions. Data-users are the entities (users/groups) that use collected data (e.g., travel expense department or tax auditor). Data-categories define different categories of collected data that are handled differently from a privacy perspective (e.g., medical-record vs. contact-data). EPAL 'purposes' model the intended service for which data is used (e.g., processing a travel expense reimbursement or auditing purposes)."

So EPAL provides for handing PII within the enterprise, not as a tool for the owner of that information. It might seem that EPAL covers the wrong end of the data exchange for our purposes here.

But the important thing about EPAL is that it removes an obstacle to corporate acceptance of PIOC by showing that there is a means for processing PIOC directions in an automated way. EPAL and related technologies make it realistically possible for companies to honor your intellectual property disclosure instructions.

Appendix 6 of The EPAL specification, which appears to be supported by the OASIS standards organization, provides a useful summary of how EPAL interacts with other privacy protocols that will be useful in implementing PIOC:

---

70 IBM Research Report, “Enterprise Privacy Authorization Language (EPAL),” by Paul Ashley (IBM Tivoli Software), Satoshi Hada (IBM Research), Günter Karjoth (IBM Research), Calvin Powers (IBM Tivoli Software, USA), Matthias Schunter (IBM Research). Edited by Matthias Schunter (IBM Zurich Research Laboratory, Switzerland), pubished May 5, 2003.

Context of EPAL (with reference to W3C's P3P, CPExchange, and XACML)

A P3P policy may contain the purposes, the recipients, the retention period, and a textual explanation of why this data is needed. P3P defines standardized categories for each kind of information included in a policy. Unlike P3P, EPAL defines the privacy-practices that are implemented inside an enterprise. Since this depends on internal details of the enterprise, it results in much more detailed policies that can be enforced and audited automatically. However, the resulting privacy guarantees can sometimes be simplified as a P3P promise that is offered for the users of the services...

The Customer Profile Exchange Specification defines a data format for disclosing customer data from one party (customer/enterprise) to another... The main focus of CPExchange lies in standardizing the data exchange format. The privacy meta-information is less expressive than EPAL. Consequently, data disclosed using CPExchange may be controlled with EPAL policies instead of using their privacy meta-data.

XACML is a general purpose and extensible access control language. Access control is a tool to define and later decide whether a user U is allowed to perform an action A on an object O. XACML lacks the privacy-specific notion of purposes. Unlike XACML, EPAL has an explicit notion of purposes and a syntax that simplifies the formalization of privacy policies..."

The implementation of PIOC can build upon a rich existing set of protocols, languages, and XML schema, making the process of honoring personal intellectual property rights very doable, at least as far as the technology is concerned. Whether that is something marketing departments want to do is another question. Some consumer activism will no doubt be called for.

What manifestations of PIOC should the consumer expect before it's built into the way our information appliances work? For starters, a site operator will need to display in a web dialog a small, unobtrusive icon that signals what sort of personal information is being captured, and what provision in your Disclosure Practice Statement makes that information capture legally permissible. You, as the author of your Disclosure Practice Statement, can change the rules at any time.

The Personal Information Ownership Component protects the privacy of all individuals. In an ideal world, that would be the end of it. But in this world we must deal with the reality of those who must be considered suspect, and whose privacy must sometimes be abridged by law enforcement in the interest of the privacy and security of others.

Now we are talking about the very definition of a slippery slope. What keeps society from sliding down the slippery slope to totalitarianism, where privacy is violated not for legitimate purposes but to allow tyrants to consolidate their power over their subjects?

One method that is sure to fail, and is therefore favored by tyrants, is to pretend that the need to pursue suspects always universally trumps the right to privacy. That's all the invitation the would-be tyrants need to concoct and pursue their plans. A real or fabricated crisis calls attention to the need to intercept the private communication of "suspects," while the absence of due process to enable that interception gives the tyrant all he needs to suspend all right to privacy in the name of national security.

Whether we like it or not, there are "suspects," that is, adversaries of tyrants, and then there are real suspects, that is, individuals whose actions suggest that they have committed, or are in the process of committing, a crime. If we deny the reality of suspects by failing to thoughtfully develop the due diligence required to define what constitutes a suspect and to intercept communications of suspects, then we play into the tried-and-true methods of tyranny.

We need another component to mitigate Quiet Enjoyment in the rare instance where it needs to be mitigated, while providing a sound mechanism for ensuring that that capability is not abused by law enforcement. We need the Accountability Component, which we cover in Chapter 22.

U-Prove Can Provide Real ZK Privacy

Of the many zero-knowledge proofs of identity, the most practical and Internet-implementable is an invention of Stefan Brands called U-Prove. Unfortunately U-Prove is too complicated to explain fully here. Fortunately, the book explaining U-Prove is available online from MIT Press[71]. Unfortunately, Microsoft purchased Credentica, the company formed by Dr. Brands that holds the intellectual property. Fortunately, as we have seen in Chapter 17, Microsoft has released much of its identity technology to open source. Unfortunately they haven't yet done that with U-Prove. Fortunately there are alternative ZK proofs of identity if Microsoft does not open source U-Prove.

Another zero knowledge proof of identity is Intel's Enhanced Privacy ID or EPID system. Intel distinguishes EPID from PKI by noting that a device such as a token, phone-wallet, or computer can authenticate by signing a challenge with an ephemeral private key that disappears after it's used, but whose corresponding public key is a "group" key. Thus the relying party can know that the person asserting identity is a valid member of the group that shares that public key, without knowing which member actually signed the challenge.

Actually ZK by itself is too good at obscuring the source of a bit stream to ensure the accountability part, which needs to be made available through the due process methods that will be described in the Accountability Component.

Whether we use U-Prove or EPID or another ZK method, the important thing is that the Privacy Commission at the City of Osmio decides what's acceptable and adopts it not just as a standard but as a municipal ordinance.

---

71 Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy, by Dr. Stefan Brands, MIT Press (ISBN 0-262-02491-8), http://www.credentica.com/the_mit_pressbook.html.

The Relationship Credential

In my book *Own Your Privacy* I introduced "old Mr. Peebles," whose understanding of your reading interests makes visits to his bookstore a pleasure. Mr. Peebles is always ready with a remarkably good recommendation for you when you drop by.

Then I showed how the Web moves the Mr. Peebles story into the horror genre, where every site seems to know not only your interests but how you think about those interests, and for that matter, how you think about everything. The next step of course is to use that knowledge to manipulate your perceptions, getting you to think the way TPC[72] wants you to think.

Relationship Credential to the rescue!

Unlike certificates that are signed by a certification authority, like Osmio VRD in our case, the relationship credential is signed by you, using the private key of your relationship signing key pair, the public key of which is signed by the Osmio VRD.

When you visit an office or outdoor site, a key pair is generated for that relationship and signed, with no effort on your part, by your relationship signing key. From then on that organization can get to know you by the public key of that relationship. You can be as friendly as you are with Mr. Peebles, but there is no way the organization can match you with other data points to learn more about you. Just as your relationship with the pharmacy next door is none of Mr. Peebles's business, your relationship with Amazon is none of Google's business.

If there is a material change in ownership of the site, the PersonalNDA and license must be signed anew by an individual who is a duly authorized representative of the new company. This prevents a repeat of the Toysmart problem described in Chapter 17.

The relationship credential is issued by, and owned by, the subject of the identity rather than by the site.

More Accountable Anonymity

The Personal Information Ownership Component includes other means of obscuring information about you while at the same time giving relying parties the assurance that you are accountable for your actions while using it.

So let's look at an example of Accountable Anonymity in social networking.

When your daughter signs up for an InDoor chat room or social network space, her computer will be asked for a certificate.

If it were a human dialog (which it isn't) it would go like this:

CHAT ROOM: Please sign this file with the key that goes with a digital certificate that shows, with a specific degree of reliability, the user's age and gender.

DAUGHTER'S COMPUTER: I can present a certificate that attests with the requested specific degree of reliability that I am a real person, and that the certificate has not been revoked.

72 See *The President's Analyst*, 1967, written and directed by Theodore J. Flicker.

CHAT ROOM: That's not good enough.

DAUGHTER'S COMPUTER: Shall I ask my user to permit disclosure of age and gender?

CHAT ROOM: Please do.

DAUGHTER'S COMPUTER: Please sign my owner's PersonalNDA.

(The PEN of the Chat Room's manager or signing officer signs the NDA.)

CHAT ROOM: Here you go.

DAUGHTER'S COMPUTER (to Daughter): The chat room has requested age and gender and has signed your Personal NDA. Shall I disclose?

DAUGHTER: Sure.

CHAT ROOM: Welcome! Please choose a username.

Sound cumbersome? Complicated dialogs like this take place between your computer and servers all the time. All your daughter has to deal with is the last question: The chat room has requested age and gender and has signed your Personal NDA. Shall I disclose? (Y/N).

She may also see this additional message:

CHAT ROOM: This certificate attests to an online enrollment procedure. We require a certificate that attests to a face-to-face enrollment. To proceed, please either make an appointment with an Attestation Officer or have a public official from your school department with an identity quality score of at least 35 sign an attestation of your identity assertion. Private school students will need to have the attestation of a notary public, justice of the peace, or a similarly empowered public official.

A reliable attestation of gender and age must involve a face-to-face session, or an attestation from an accountable person who knows the subject.

Different Quality Strokes for Different Folks

"Identity quality" means different things to different relying parties. Parties in a large financial transaction are more concerned with whether the certificate carries bonding against fraud than with the age of the subject.

Only necessary information is disclosed, and only under NDA and license. With the Personal Information Ownership Component, the only piece of information that is disclosed by default is this:

> This computer or phone is under the control of a real human being who presents an unrevoked digital certificate that carries an identity quality score of __.

Osmio's Vital Records Department is the authoritative source of unchanging information about this person. The Vital Records Department and the Privacy Protection Department represent public authority and are trusted to disclose that information only to entitled parties, and only under certain circumstances.

Typically that party is the subject of the certificate and the circumstance is an authenticated request. But the request may also be from a police department and it may include a court order.

That leads to another question: “Which police and which courts In the physical world the vital records department can be a unit of a national government, and sometimes not a trustworthy national government. There has to be a way to ensure that the certification authority itself strictly adheres to regulations governing disclosure. It's called putting all the identity eggs in one basket. The Personal Information Ownership Component and the Authenticity Infrastructure of which it is part allow us to effectively watch the basket.

Osmio's city hall and its vital records department have nothing to do with any existing government or physical jurisdiction. Your second home, your online residence, is in a community that consists of people who have chosen to have the benefit of authenticity.

Who governs city hall?

You do.

It’s your municipality; if you're a resident, you own it.

Who watches the identity basket? You and your neighbors, particularly those who serve on the city's Certification Practices Commission.

Covering Your Fingersteps: Part Two

We've shown how the Personal Information Ownership Component protects sources of your personal information that you know about, that is, the formal information about yourself.

What about the information about you that's collected by the cookie clubs that watch you without your knowledge, aggregating your site visit data and clickstream data and cookie data so they can sell it to political parties and marketers and, well, there's no way of knowing who they sell it to and share it with?

We call those groups the cookie clubs.

The remarkable thing is, there is no one essential piece of information in the clump of information that uniquely identifies you, even though the whole clump identifies you precisely. When it comes to identification, the clump of information about you is just like the physical you.

The physical you does not need to have a name or ID number embedded somewhere in your organs or bones in order for you to be the unique you.

Let's demonstrate by way of a thought experiment. Imagine that 100 years from now science develops a means of determining, just by examining an object, the DNA of everyone who has touched that object, and the time it was touched. The technique is so good it can do that with objects touched 50,000 years ago, before there was any such thing as recorded information.

Using that technology and the technology of database tables, joins and queries, you would be able to construct a very complete record of the life of any individual who lived back then.

That thought experiment should show why a social security number or other national ID or even a name is totally unnecessary for the cookie clubs to know that that info clump is the digital you.

The info clump that constitutes the digital you takes the form of tables produced by table joins from many, many sources.

The cookie clubs don't need an identifier in order to deliver to their clients and fellow club members a very accurate picture of you, your habits, your preferences, your political leanings, your buying habits, your vulnerabilities.

Anonymity is called for. Anonymity does not imply anything improper on the part of people who choose not to disclose their identity, regardless of what Eric Schmidt might say on the subject. Lots of people like to have different usernames in different places, to keep them from being tracked when they don't want to be tracked.

But anonymity is trickier to establish than may first appear. There's more to it than simply installing an anonymizer in your computer or going to the web through an onion router such as the Tor system provides. We've noted that your computer and phone are full of files placed by people who want to track you, regardless of whatever username you happen to be using, which rather defeats the attempt to remain anonymous and untracked.

Before we get to deep, thorough anonymization, let's remember that while we want to be completely anonymous, we want those we deal with to be accountable. If that 11-year-old girl in a chat room with your daughter is actually a 50-year-old predator, you'd like to know that. If that laptop you bought in an online auction seems to be late in arriving, you'd like to know that the seller is an identifiable human being.

And you'd like some accountability from the person spreading false rumors about your family in Facebook.

We rely on the assertions made by others, and so we all want accountability. At the same time we want privacy, which can mean anonymity. We want both anonymity and accountability at the same time. And we can have just that through the Personal Information Ownership Component. As we pointed out, it's like the anonymous accountability we're supposed to have with car registrations. Everyone can see your license plate number, but others can't know your identity except under certain circumstances.

There has to be a back office whose practices and policies are visible and monitorable and at the same time secure.

As you own your identity, you should own the authority that issues your identity, just as you own the city where you live and the vital records department that issued your paper birth certificate.

With the physical license plate on your physical car, it takes considerable effort for governments and marketers to keep track of where you go. But on the information highway it's fairly easy< for nosy organizations to track your every fingerstep. Your habits, your social and political relationships, your place of residence – everything is easily discoverable and is constantly recorded in tables that are relentlessly joined with other tables about you from other sources.

Unlike the physical highway where nosy organizations find it impossible to track your every move, on the information highway it's quite possible. So we need to take other steps.

So once again we need to examine our assumptions about the Internet. We're used to saying things like “the browser appears in a window...” Well, what's a browser and what's a window?

A window is something that allows people to see the outdoors, of course. From indoors.

That's the legitimate use of a window. Looking the other way, from outdoors to InDoors, is typically not legitimate.

When you go from place to place inside one of our InDoor spaces, you do not need a browser. After all, you don't use a vehicle and a GPS to navigate inside a building. Rather, the relationships between spaces in the building are defined by corridors.

In an InDoor space there is no need for DNS or URLs or for that matter Web addresses, because our buildings are apart from the highway InDoors is not on the Web.

InDoors provides no facilities for those outside our windows to look in on us and track what we are looking at.

From an InDoor space you can enter a url and browse outside to your heart's content. But if you want to do your online banking either the bank will need a building to which you have InDoor access, or you'll need to go outside to do your banking on the Web. Yes, that web, with all its phishing sites with no occupancy permits, accessed via browsers running in a space made by code that no professionally licensed code auditor has looked at. Good luck out there.

I'd like my bank to have a building rather than keeping my money in boxes on the sidewalk. If no such InDoor banks exist, well, perhaps you know of an entrepreneurial banker who would like to start one.

Stepping outside of our metaphor for a moment, the technology for browsing from InDoors consists of two things. The first is software called a “door,” which looks like a browser

but which has no ability for a site to put anything on your machine. Basically it's a browser with no address bar, no JavaScript, no cookies and no such other elements of outdoor space. Its code is digitally signed by a professionally licensed architect, contractor, and building inspector, each of whom attests to its being free of back doors or hidden agendas.

Covering Your Fingersteps: The Last Mile

But still, the Net itself provides a means for tracking your packet vehicles on the highway, even if those packets are only used from within InDoor spaces. Here the answer is available off the shelf.

It's good old Tor anonymization software. Because after you've eliminated all the internal tracking mechanisms, you still need to obscure your IP address. Tor, or other onion routing software, is therefore part of the viewer software.

Tor stands for The Onion Router. Originally sponsored by the Electronic Frontier Foundation using technology developed for the U.S. Navy, the Tor client, which is built into Dorren client software that presents InDoor spaces, routes Internet traffic through a global network of onion router servers that hide the user's IP address and location.

Onion routing is designed to make it difficult to trace "visits to Web sites, online posts, instant messages and other communication forms." It's called “onion routing” because of the way the data is encrypted at each independently-operated node, as suggested by the layers of an onion. If one node is compromised, it's assumed that at least one other node will not be.

Summing It Up

By doing things InDoors you're eliminating one source of fingersteps information. The ZK Credentials and Rental Credentials and Relationship Credentials take care of another. And finally there's Tor to sweep clean those last traces of your travels around the world's information infrastructure.

There’s also accountability through due process. Let's now take a look at how the Accountability Component portion of the Quiet Enjoyment Infrastructure accomplishes that.

To see the current state of development of

The Personal Information Ownership Component

…and to learn how your

experience with zero knowledge proofs

might be put to use in its development, please go to the Personal Information Ownership Component Development Office at osmio.ch