PERSONAL DATA JOURNAL

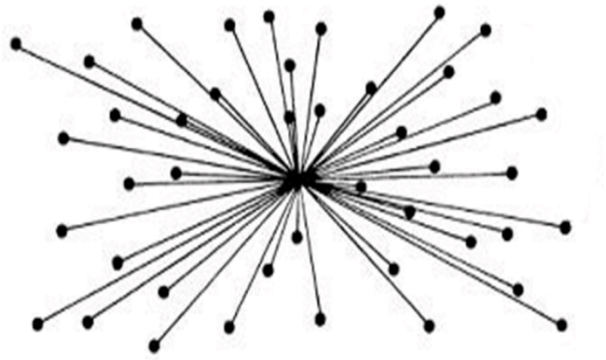
Issue N°3 April, 2012

Personal Data in Decentralized Network Architectures

by Markus Sabadello, Technical Editor

One of the most fundamental challenges for the PDE to consider will be the design and deployment of suitable underlying architectures for realizing emerging visions around the management and use of personal data. The basic organizational structures, according to which participants of an ecosystem exchange information with each other, influence many of its fundamental properties, such as privacy, security, flexibility, discovery, or the dependencies between different actors. The possible types of architectural patterns that can be implemented are highly diverse, with centralized structures on one end of the spectrum, and fully distributed systems on the other end. On the Internet, very different forms have always existed, depending on the infrastructural layer and the concrete applications and services one looks at.

Such organizational structures can be described and analyzed using terminology and methods from the mathematical field of graph theory. They are really trans-disciplinary concepts, which have been applied to many practical situations and academic theories both in the natural and social sciences. One often-cited book in this context is "Neither Market nor Hierarchy: Network Forms of Organization" by Walter W. Powell (1990), which argues that with the advent of modern communication technologies, decentralized networks have become an increasingly important concept in various disciplines. Today, they are used not only to describe certain electronic communication systems, but also the structures of corporations, international relations, terrorist organizations, revolutionary movements, and civil society.



Centralized Architectures

Centralized architectures are based on the idea that all communication passes through a single point in the system, which is responsible for managing the flow of information between participants, for coordinating their behavior, and for

Contents

Feature Article: Personal Data in Decentralized Network Architechures , Page 1

Industry News: Page 3

Events: Page 6-7

Standards: Page 8-9

Startup Circle: Page 10

Resources: Page 11-12

Special Report: US Privacy Initiatives, Page 13

Book Reviews: "The Daily You" and "Consent of the Networked," Page 14-15

Opinions: Sara Wedeman and Tony Fish, Page 16-17

Publisher's Note: "Catalyzing the Ecosystem," by Kaliya Hamlin, Page 22

Editorial: "US and EU: A Tale of Two Cities," by Kelly Mackin, Page 27

introducing hierarchies. This approach has the advantages of being efficient, well organized, reliable, and secure, as long as all key components of the hierarchy function correctly.

In practice, this means that these systems make use of central hubs or servers, which transmit, control, and organize all information and all communication within the system. Such designs are known as client-server architectures, or more recently described with marketing terms such as "software as a service" or "cloud computing". Today, many of the most widely used Internet services such as Google Search, Gmail, Facebook, Twitter and Youtube are based on this design, involving a powerful server structure at the center of the architecture, and large numbers of clients on the periphery which depend on instructions and information from the servers.

The implication of such centralized systems is that the political or corporate entity offering a service is in full control of all personal data and communication processes which take place, and as a result, there is an inherent potential for abusing this control and for violating the privacy of participants. Concrete abuse scenarios and harmful consequences include the excessive storage, analysis, aggregation, manipulation, and monetization of personal data, as well as the surveillance and manipulation of people's messages as they are exchanged via a network. And besides general privacy issues, which are shared by large numbers of users, concerns have also clearly increased as a consequence of political events such as the Iran Green Revolution, the Arab Spring, Tea Party or the Occupy Movements, where activists often found their online communication to be monitored, censored, and used against them by established political authorities.

As a consequence of strong tendencies toward more centralized and strictly hierarchical designs of online applications and services, criticism has become widespread. With growing public awareness about the deficiencies of highly centralized systems, the search for alternatives has also intensified, and various countertrends have emerged. To some extent, tools such as Encrypt Facebook or CrypTweet can be used to achieve more privacy; however, they are really just workarounds. The real alternative – i.e. adopting decentralized architectures – is now more popular than ever before, and visions as well as concrete projects to enable personal data storage and communication in decentralized network architectures are on the rise.

Decentralized Architectures

Alternatives to centralized forms of organization are commonly referred to by the terms "decentralized", "distributed" or "peer-to-peer", and they provide communication structures that are less or not at all dependent on any single central point in the system. Therefore, there is an inherent potential to give individual participants more control, privacy and independence. Some approaches exhibit certain hierarchical features (e.g. "federations" that still distinguish between clients and servers), whereas others are completely distributed and do not distinguish between different participants in any way.

Personal Data Journal

Personal Data Journal is published by the Personal Data Ecosystem Consortium. Our goal is to create and support a diverse community of companies, small and large around the world building a thriving personal data ecosystem.

Personal Data Journal Staff

Publisher: Kaliya Hamlin
Associate Publisher: Patrick Reilly
Editor: Kelly Mackin
Technical Editor: Markus Sabadello
Researcher: Joseph Boyle

Sales

Patrick Reilly pat@pde.cc

Subscriptions:

Enterprise licenses for Personal Data Journal are available at http://www.pde.cc/journal for $3,000 - $10,000 depending the organization's size.

Personal Data Journal is published by **Personal Data Ecosystem Consortium** a non-profit 501(c)6 trade association.

Executive Director:
Kaliya Hamlin

Board Members:
Clay Shirky
Phillip J. Windley, Ph.D.
Tony Fish
Aldo Castaneda

http://personaldataecosystem.org

Decentralized networks offer greater resilience against disruptions and they are effective in repairing topological damages due to redundant and re-adjustable connections between participants. Their ability to easily add and remove new connections enables them to recruit and integrate new members into the network at any time, or to even join separate networks together. Yet another strength of such networks is their ability to transmit and process messages in a very efficient way, bypassing hierarchies that may cause obstruction and delays, and getting information directly to the participants that need it. Connections between participants can be dynamically optimized, and resources or communication channels that are found to be valuable can immediately be used again.

One of the ideas that is currently receiving a lot of attention is to build a decentralized social networking service, i.e. a "Facebook without a single Facebook", or in other words, an infrastructure similar to E-Mail, where multiple service providers and users can interact with each other and fulfill their social communication needs, without being dependent on any single company or server system. Based on this idea, the Federated Social Web effort has emerged, which operates as a W3C Community Group and has so far held two summits in Portland, Oregon, and Berlin, Germany. A web comic exists that explains the idea in simple terms, conferences dedicated to decentralized architectures such as Unlike Us are being held, and Wikipedia currently lists about 50 distributed social networks.

The following is a list of currently active projects that aim to build decentralized architectures for working with personal data and communication. Some of them have had a stable codebase for years and have successfully built large user communities.

Diaspora, one of the most prominent projects, has raised USD 200,000 via the Kickstarter crowdfunding platform to implement a decentralized social networking service.

StatusNet is a decentralized microblogging service that uses the OStatus federation protocol for interoperation between different instances.

RetroShare provides serverless, encrypted chat and file transfer services, and relies on a web-of-trust to authenticate peers.

Tribler is a BitTorrent client developed by the Delft University of Technology. Several projects are underway that attempt to use its kernel component Dispersy for purposes other than file sharing, for example encrypted messaging and newsfeeds.

SocialSwarm sees itself not as a software project, but as an advocacy group that can act as a mediator between different initiatives.

Unhosted attempts to decouple applications from data storage by providing an abstract "remoteStorage" API, therefore giving individuals choice and eliminating the need for being dependent on any single part of a system.

SecuShare provides social networking that is completely independent of servers and instead relies on client software communicating in a peer-to-peer fashion. It implements a "social onion routing" protocol that utilizes one's social graph for routing purposes and for calculating trust.

Thimbl uses the Finger technology from the early days of the Internet to enable decentralized microblogging, and it makes a strong political statement by describing capitalism as the reason why today there is too much centralization online.

Crabgrass provides tools for organizing and collaborating in democratic ways. However, it does not view itself as a traditional social network. It focuses on group collaboration rather than a hierarchic, ego-centric approach.Briar seeks to develop a secure communications network for civil society tat can use different underlying infrastructure and even operate outside of the Internet. It also tries to incorporate a new sense of sociality rather than simply rebuild existing social networking services.

Lorea (Basque for "flower") also works on free and federated decentralized social networking for civil society. It includes components for discovery, decision making, and new social economic models.

The FreedomBox Project

The FreedomBox is one of the most interesting projects that try to implement decentralized communication patterns on the network level. Some of the following information is based on a presentation of FreedomBox Foundation executive director James Vasile at the Elevate 2011 festival in Graz, Austria, as well as on a lightning talk at the 28th Chaos Communication Congress in Berlin, Germany.

(Continued on Page __ See *FEDERALIZATION*)

NEWS

Marketing is the New IT

"By 2017, a CMO will spend more on IT than the CIO." —Gartner Group

For the first time in history, businesses can leverage big data for the benefit of driving marketing insights. We are at the very beginning of this wave, but this fundamental shift will create several multi-billion dollar winners. And a set of technology companies will emerge as the marketing equivalents of Salesforce and SAP."

[Get ready, folks. - Ed.]

http://gigaom.com/2012/03/17/marketing-is-the-next-big-money-sector-in-technology

Text Messages Would Become Protected in S'pore

Singapore is moving ahead to include cell phone text messages under introduced privacy legislation. With cell phone companies globally selling and forwarding text based content. This is a notable event.

http://news.asiaone.com/News/Latest%2BNews/Singapore/Story/A1Story20120320-334439.html

Microsoft's Life Browser lets you Digitally "Harken Back."

Like a photo album taking you back to the smell of mommy's brownies, The Microsoft Life Browser assembles your social and personal documentation so that you can replace the photo album with a browser.

http://www.technologyreview.com/computing/39917/?ref=rss

Facebook's Permanent File on You

All of our readers are aware of a seemingly pernicious quality to Big Data policies. Unlike high school, where the "permanent record" went to the shredder decades ago, Big Data's unending hunger for more data is bound to affect people's lives both negatively and perhaps positively in some instances - but whose choice is it?

http://kiwicommons.com/index.php?p=11268&tag=extensive-user-data-kept-by-facebook-indefinitely

Time.com Says that "People are Cheapskates" When it Comes to Protecting their Data

"The value of consumers' personal data online has been a hot topic lately. The astronomical $100 billion some analysts have suggested Facebook could be worth when it goes public stems from the fact that the social media powerhouse has reams of data on users' chatting, browsing and buying habits. But we're so short-sighted we won't pay more to protect that data — even if the cost of that protection is a measly 65 cents."

http://moneyland.time.com/2012/03/19/were-total-cheapskates-when-it-comes-to-our-privacy/#ixzz1qGRxFFn0

Personal Data Solutions Coverage of Startups from SXSW

Here's a good roundup of coverage from SXSW. -Ed

http://news.idg.no/cw/art.cfm?id=7F3D70F5-D59F-70A1-22B76471C46E9F96

Big Government Moves on Privacy

With the White House announcement of the Consumer Bill of Rights, a flurry of additional activities have taken place. (CBA is covered here in the Features section). An EU delegation has traveled to Washington and interestingly the EU referred to the US and EU as an evolving "Common Market." We had not heard that before... Additionally, the FTC announced the final version of their privacy report; and Senators Kerry and McCain introduced legislation called The Commercial Privacy Bill of Rights Act of 2011. It's been a busy March.

FTC: Privacy Report:

http://www.ftc.gov/opa/2010/12/privacyreport.shtm

Congressional Bill:

http://kerry.senate.gov/press/release/?id=59a56001-5430-4b6d-b476-460040de027b

EU/US Joint Statement on Privacy:

http://www.marketwatch.com/story/eu-us-joint-statement-on-data-protection-by-european-commission-vice-president-viviane-reding-and-us-secretary-of-commerce-john-bryson-2012-03-19

Consumers Not Loving the Targeted Advertisements

"The research found that just 16% of the 2,276 UK consumers polled said they were positive to the idea of using personal data to lead to better and more targeted advertising messages. Similarly, just 15% said they were positive to the use of their browsing history to provide more targeted advertising."

http://www.marketingweek.co.uk/news/consumers-still-cold-to-the-idea-of-targeted-ads/4000605.article

Edelman Study: People Sense that they Have No Control Over Biz Use of Info

An interesting Privacy and Security Slideshow with Lots of Data.

http://www.slideshare.net/EdelmanInsights/privacy-security-the-new-drivers-of-brand-reputation-and-action-11906743

And a Story on It...

http://www.mediabistro.com/prnewser/research-68-percent-feel-they-have-no-control-over-the-way-businesses-use-personal-info_b35183

Personal Medicine Emerges with Startup and your DNA

http://www.telegraph.co.uk/finance/businessclub/9141838/Data-firm-sees-gold-mine-in-personal-medicine.html

James Temple on Do-Not-Track

"Late last month, the Digital Advertising Alliance and Google made headlines by committing to incorporate do-not-track technology that promises to give users greater control over how their online information is used. But privacy advocates and more recently several regulators have expressed concern that..."

http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/03/06/BUMC1NG94D.DTL#ixzz1qGpFUZDZ

American Express Pushes Hard for Links to User Twitter Accounts

American Express wants to link Card accounts to your twitter account. The connection would be a gold-datamine for the company because it would enable them to plum the relationship of card activity to the TweetStream.

http://www.readwriteweb.com/archives/amex_offers_discounts_to_customers_who_link_cards.php

Spanish Court Refers Google Case to ECJ for Publishing Obsolete and Embarrassing Data

Audiencia Nacional, a Spanish Court, has some 130 similar cases pending before it, in which Google is appealing injunctions issued by the Spanish Data Protection Authority against the search engine.

https://ispliability.wordpress.com/2012/03/02/spanish-court-asks-the-ecj-whether-google-must-delete-links-to-personal-data/

Note that the Regulation containing the formal right to be forgotten is not in force yet. This is all on the basis of current legislation, not on the basis of the reforms under way.

Recent Pew Report on Hyperconnected Lives

"Teens and young adults brought up from childhood with a continuous connection to each other and to information will be nimble, quick-acting multitaskers who count on the Internet as their external brain and who approach problems in a different way from their elders, according to a new survey of technology experts. This study is covered in more detail in the Resources Section.

http://pewinternet.org/Reports/2012/Hyperconnected-lives.aspx

Cloud Connected Credit Card + Health Data?

"The "quantified self" is an emerging trend in the digital health space. Early adopters and fitness buffs are wearing devices like Fitbits and Nike FuelBands to track their heart rates, calories burned, quality of sleep and more, so that they can measure and improve their health and performance. The cloud-connected credit card will also deliver a stream of valuable intelligence based on your transaction behavior. Your health data stream alone could include how much of your diet is fast food, how often you actually visited your health club, and how many times you stopped for coffee (aka "your caffeinated self"). Your appified card can also deliver you informed insights on your spending activities across other life categories so that you can optimize decisions and be your best self."

http://www.forbes.com/sites/bruceupbin/2012/03/01/the-credit-card-is-the-new-app-platform/

What Could be Worse than a Government Issued ID? A Facebook or Google one?

An Art Project by a European Artist is Tweaking People Across the Globe.

http://m.zdnet.com/blog/facebook/get-your-own-facebook-google-id-card/9671

Australian IIW Write Up in ZDNet

Kaliya Hamlin went to Australia in March and spoke at Digital Identity World about the spectrum of Identity and the Personal Data Ecosystem. Stilgarian wrote his impressions of the Internet Identity Workshops she facilitated a few days later.

http://www.zdnet.com.au/the-facebook-experiment-339334444.htm

Events

Bolded events in Black *were not listed in previous issues.*

Data 2.0 Summit

April 3, 2012

San Francisco, CA

http://data2summit.com/

PDEC staff are attending - highlights will be in the May Issue. - Ed.

WSJ Hosted Data Transparency Weekend

April 13–15, 2012

New York

datatransparency.wsj.com/

Code-a-thon to develop tools. Personal is sponsoring this event.

Data Usage Management on the Web at WWW 2012

April 16, 2012

Lyon, France

dig.csail.mit.edu/2012/WWW-DUMW/

Data usage control generalizes access control in order to address what happens to data in the future and after it has been shared or accessed. Spanning the domains of privacy, the protection of intellectual property and compliance.

European Identity & Cloud Conference

April 17–20, 2012

Munich, Germany

www.id-conf.com/

This is the premier spring conference in Europe covering these issues. Patrick Reilly the Associate Publisher of PDEC and Markus Sabadello the technical editor of this publication will both be at EIC along with Phil Windley who is on our board. Several of the startups from both North America and Europe will be there and you can contact us if you have employees attending who you want to meet up with the community.

Doc Searls is curating the following sessions with leading thinkers, builders and key new developments in European thinking.

The Life Management Platforms

http://www.id-conf.com/sessions/1026

Giving Individuals Control and Knowledge of their Personal Information held by Others - What are the Consequences?

Prof. Dr. Kevin Cox, Edentiti

Scott David, K&L Gates LLP

Tony Fish, My Digital Footprint

Marcel van Galen, Qiy

Drummond Reed, Connect.Me

Trust Frameworks - Internet Identity - Life Management Platforms

Drummond Reed, Connect.Me

Markus Sabadello, XDI.ORG

Phil Windley, Kynetx

This roundtable will examine the role of socially-verified trust networks in the emergence of Internet identity and the personal data ecosystem.

The GINI-SA Project of the EU

Lefteris Leontaridis, NetSmart S.A.

GINI-SA is a Support Action for the EC which aims to analyze how a Personalized Identity Management (PIM) ecosystem in which individuals can manage their own digital identities and control the exchange of their identity information.

Under the GINI vision, individuals would manage their identities by means of an Individual Digital Identity ('INDI'). An INDI can be described as a self-generated and self-managed digital identity, which is verifiable against one or more authoritative data sources.

Once created, users would have the ability to link their INDI with authoritative identity data maintained by both public- and private-sector entities. This data (or links thereto) could then be presented by the user towards relying parties. The user might wish to do this in order to meet transactional requirements (e.g., access control conditions set by a relying party) or underpin her trustworthiness towards others in various real life situations (e.g., verifying her education or presenting her skills when applying for a job).

The main objectives of GINI include:

1. Decoupling the activation of digital identities from the use of any particular identifier, and to support the use of multiple identities and/or identifiers;
2. Allowing users to exercise full control as to who is able to verify her identity and through which processes;
3. Enabling user control every phase of their digital identities' life cycle (creation, change, management, revocation, etc.);
4. Identifying the ways and means through which a separation of identifiers and other identity attributes can be implemented in a user-friendly manner;
5. Outlining the main properties of a digital identity ecosystem that is efficient and yet capable of enabling maximum control of users over their digital identities;
6. Determining the prerequisites for operators so that a viable business model can be established.

GINI further examines the technological, legal, regulatory and privacy-related dimensions of the gap between the current state of the art and the vision for a functional INDI ecosystem beyond 2020. Detailed examinations of these gaps have been carried out in the individual work packages of the project. The following sections briefly introduce the major gaps identified thus far.

The aim of this presentation would therefore be to engage stakeholder representatives from the policy and industry domain and exchange views that will be taken into account for the formulation of the White Paper and Roadmap GINI will publish within 2012.

Internet Identity Workshop

May 1–3, 2012

Mountain View, CA

www.internetidentityworkshop.com/

This is also PDEC's main convening opportunity and it is global in nature. Key European innovation and thought leaders in the space and they are planning to attend the event. We strongly encourage all those interested in making the ecosystem real attend.

VRM and CRM Inter-op

April 24, 2012

London, UK

Price: £20

http://www.eventbrite.com/event/3198405517

VRM and Personal Data Services are emerging with increasing regularity, and various components of the Intention Economy eco-system are falling into place. But, by default, these services will have to interact and inter-operate with each other to meet an individuals needs, rather than seek to be a silo solution. This event is aimed at developers and architects of 'VRM' services looking to test and evolve how their services inter-act and inter-operate with other components of the VRM eco-system, and to test and evolve connections between person-centric VRM services, and organization-centric CRM services and applications.

IPSI SmartData International Symposium

May 14–16, 2012

Toronto, Ontario, Canada

www.ipsi.utoronto.ca/sdis/

This event was brought to our attention by Ann Cavokian the Privacy Commissioner of Ontario who has been leading the Privacy by Design movement. -Ed.

The future of privacy, and, in turn, our freedoms, may well depend on the ability of individuals to reclaim personal control of their information and identities online.

SmartData is a vision to create Internet-based virtual agents which will act as an individual's online proxy to securely store their personal information and disclose it based upon the context of the data request and instructions authorized by the data subject.

Web 2.0 Security and Privacy Workshop

May 24, 2012

San Francisco, CA

www.w2spconf.com/2012/

This workshop is co-located with the IEEE Symposium on Security and Privacy (below). The goal of this one-day workshop is to bring together researchers and practitioners from academia and industry to focus on understanding Web 2.0 security and privacy issues, and to establish new collaborations in these areas.

IEEE CS Security and Privacy Workshop

May 24-25

San Francisco, CA

http://www.ieee-security.org/TC/SPW2012

Conference on Web Privacy Measurement

May 31– June 1, 2012

Berkeley, CA

www.law.berkeley.edu/12633.htm

Hosted by the Berkeley Center for Law & Technology. Studying tracking technologies.

European e-Identity Management Conference

June 12-13, 2012

Paris, France

Cost: €220-€770

www.revolution1.plus.com/eema/index.htm

Business, public sector and government who are involved in policy, security, systems and processes.

Cloud Identity Summit

July 17-21, 2012

Keystone, Colorado (near Denver)

http://www.cloudidentitysummit.com

This event hosted by Ping Identity and lead by its CEO Andre Durand is unique for its high quality of presentations and attendees along with its family atmosphere. There were over 100 families in attendance - Andre's wife organizes a whole series of family activities in the day time and evening meals are with everyone together. The event leans towards an enterprise focus but will cover topics around identity and personal data.

OSCON (Open Source Convention)

July 17-21

Portland, Oregon

http://www.oscon.com/oscon2012

This O'Reilly event is the heart of the open source world and draws people from around the world. Open Standards are a key aspect of the event Federated Social Web get work done in F2F meetings during this event. There are several open source projects in PDEC I (Kaliya) expect they will present/be covered at this event.

New Digital Economics London

June 12-13, 2012

London, UK

www.newdigitaleconomics.com/EMEA_June2012/

(SOUPS) Symposium on Usable Privacy and Security

Date: July 12–13, 2012

Washington, D.C.

cups.cs.cmu.edu/soups/

Paper deadline March 9.

Cost: $100–$400

Chip-to-Cloud Security Forum

September 19–20, 2012

Nice, France

http://www.chip-to-cloud.com/

"From smart cards to trusted mobile and Internet of Things"

Abstract deadline March 23.

SIBOS

September 19–23, 2012

Osaka, Japan

http://www.sibos.com/osaka.page

€950/day, €2800/week

This is the annual gathering of SWIFT the international bank messaging cooperative. Kaliya has presented to them a number of times and they are proactively involved in understanding the way traditional banks and banking networks can play a role in the emerging ecosystem.

Standards

OpenID Connect: Implementer's Drafts Approved

Feb 17 2012

In the vote held from February 7-15, 2012, members of the OpenID Foundation approved the following OpenID Connect specifications as "Implementer's Drafts":

- Basic Client Profile – Simple self-contained specification for a web-based Relying Party. (This spec contains a subset of the information in Messages and Standard.)
- Discovery – Defines how user and provider endpoints can be dynamically discovered.
- Dynamic Registration – Defines how clients can dynamically register with OpenID Providers.
- Messages – Defines all the messages that are used in OpenID Connect. (These messages are used by the Standard binding.)
- Standard – Complete HTTP binding of the Messages, for both Relying Parties and OpenID Providers.
- Multiple Response Type Encoding – Registers OAuth 2.0 response_type values used by OpenID Connect.

Out of 363 members, 86 voted in favor, 1 voted against, and 2 abstained. An Implementer's Draft is a stable version of a specification providing intellectual property protections to implementers. Within the PDE, OpenID Connect is a likely technology to be used for identity and the sharing of personal data.

OAuth 2.0: Threat Model and Security Considerations

Feb 19 2012

An Internet Draft (version 02) containing an OAuth 2.0 Threat Model and Security Considerations has been submitted by the IETF Web Authorization Protocol Working Group. It contains a long list of approximately 50 different threats that can affect all actors at various stages of the protocol. It lists and explains comprehensive counter-measures to deal with these threats, and it describes the built-in security features of OAuth 2.0.

http://www.ietf.org/id/draft-ietf-oauth-v2-threatmodel-02.txt

SCIM: Use Cases

Feb 23 2012

The Simple Cloud Identity Management initiative (SCIM, formerly also known as "Cloud Directory") is developing concrete use cases which are to be used as the basis for an upcoming interop event on March 25 2012. SCIM aims at creating a schema and API for making personal data of individuals and organizations portable between websites. The use cases include classic CRUD operations such as creating, updating or deleting a user. Although SCIM is at this time not yet widely used, it is specifically designed to promote interoperability between heterogeneous systems and could therefore potentially be a building block for the emerging PDE.

IETF: "privacy-policy" Link Relation Type

Feb 23 2012

In an Internet Draft (version 01) submitted to IETF, three new Link Types for Web Linking are defined: "implements", "privacy-policy" and "terms-of-service". Web Linking is a universal framework for expressing typed relations between web resources, and it can be used in various ways, such as in HTTP headers, HTML or ATOM elements, or by the XRD descriptor format. This framework is originally specified in RFC5988, which also contains several initial Link Types, such as "copyright", "license" or "payment". The introduction of "privacy-policy" as a new Link Type provides a standardized way for documents and other web resources to declare a privacy policy associated with its contents. The privacy policy can be any resource that discloses what personal information about the user is collected, and how that personal information is stored, used, managed and disclosed to other parties. This only serves informational purpose, and there is no mechanism to provide guarantees or control.

A "privacy-policy" Link Type could be highly relevant for a PDE in which privacy of personal data is a key goal. The two other new Link Types, "implements" (which can be used to declare compatibility with a certain standard) and "terms-of-service" (to point to a Terms of Service document) could also be useful for use cases within the PDE.

http://www.ietf.org/id/draft-snell-additional-link-relations-01.txt

OASIS ID in Cloud: Public Review for Identity in the Cloud Use Cases Version 1.0

Feb 25 2012

The OASIS Identity in the Cloud TC has produced an updated Committee Note Draft and submitted it for 15-day public review. This document is intended to provide normative use cases that examine the requirements of identity management functions as they are applied to any cloud deployment or service model:

Identity in the Cloud Use Cases Version 1.0

Committee Note Draft 02 / Public Review Draft 01

http://www.oasis-open.org/committees/download.php/45281/id-cloud-usecases-v1.0-cnprd01.zip

OASIS WSS-M: Public Review for Web Services Security Candidate Version 1.1.1

Feb 28 2012

Members of the OASIS Web Services Security Maintenance (WSS-M) TC have approved a Special Majority ballot to advance Web Services Security Version 1.1.1 Committee Specification 01 to Candidate OASIS Standard (COS). The COS now enters a 60-day public review period in preparation for a member ballot to consider its approval as an OASIS Standard. Web Services Security Version 1.1.1 is a multi-part specification consisting of seven different parts.

W3C TAG: Amendment for httpRange-14

Feb 29 2012

A call for proposals to amend the W3C TAG's famous httpRange-14 resolution of 2005 has been issued. This resolution - which has been a highly controversial topic in the web community throughout the years - states that HTTP URIs may be used not only to identify documents on the web, but also any arbitrary resources such as people, cars, or abstract concepts. This has had deep implications on how RDF, Linked Data, and the Semantic Web in general function. The decision to possibly amend it could therefore also have a direct impact on the vision of an interoperable PDE, in which many initiatives today already base their architecture on URIs, RDF, and other fundamental building blocks of the web.

New PMRM Draft

March 6 2012

The OASIS Privacy Management Reference Model (PMRM) TC has published a new draft version (Working Draft 03) of their main deliverable. This TC works to provide a standards-based framework that will help business process engineers, IT analysts, architects, and developers implement privacy and security policies in their operations.

New XACML Draft

March 19 2012

Nearly one year since the last version, the OASIS eXtensible Access Control Markup Language (XACML) TC has published a new draft version (Working Draft 23) of their core specification. XACML defines a core XML schema for representing authorization and entitlement policies. Although functional changes are minimal, implementers should take a look at the list of changes in this new draft.

Privacy by Design in APIs

March 29 2012

The W3C TAG has begun work on a draft finding on the topic of "Privacy by Design in APIs". It is intended to provide strategies for API designers to be as privacy-friendly as possible, especially when it comes to fingerprinting and the minimization of information while using JavaScript APIs. This is another one in a series of efforts by standards bodies to address the large topic of privacy in web applications. Other such efforts include the IETF documents "Privacy Terminology and Concepts" and "Privacy Considerations for Internet Protocols", the W3C Privacy Interest Group (itself part of the W3C Privacy Activity), and the IETF Privacy Program.

OpenID Connect: Test Lab

Mar 21 2012

European research project GÉANT has deployed an OpenID Connect Test Lab, which can be used to test an OpenID Connect Provider. This is an early preview of a bigger set of components, and its functionality is explained in detail in a video.

UMA Revision 4

March 30 2012

A new revision of the User-Managed-Access protocol (UMA) has been published. UMA builds on OAuth and is based on the idea of providing a centralized interface through which individuals can manage all their authorization, sharing and service access. The new revision adds examples and several new subsections, e.g. about the UMA bearer token profile and the OpenID Connect claim profile.

http://docs.kantarainitiative.org/uma/draft-uma-core.html

Startup Circle News

Personal.com's writeup on their presence at SXSW is a worthy read

"A deluge of rain welcomed the Personal team to Austin two weeks ago today. Armed with company swag and a passion for spreading the word about small data and our product, we went to battle with the weather."

http://blog.personal.com/

Personal led a panel discussion on the Digital Bill of Rights that they have created. They covered the topic of monetizing personal data in a panel about "Data is the New Oil." They covered the scandal on cookies and web privacy, and a panel on Big Data: "Privacy Threat or Business Model."

Connect.Me

Ten Words for Trust

After a six week bootstrap period, today marks the full start of Trust Anchor vouching on the Connect.Me private beta. Trust Anchors are the highest of the four trust levels in the Respect Trust Framework. Only Trust Anchors can give a Trust Anchor vouch. This blog post explains the framework:

Connect.me has opened spots for the first of nearly 700 so-called Trust Anchors to join them in a Ten for Trust blog post. The effort is designed to get people to put into their own words what a trust anchor means.

http://blog.connect.me/ten-for-trust/

is proud that today they released LinkedIn as their third service with which you can connect to Archify.

Archify is a service that allows people to capture their social streams and social web activities. It integrates with any browser.

http://blog.archify.com/welcome-linkedin

MyDex Expands Team

"Mydex is pleased to announce that David Brewer and Diana Jeater are joining the Mydex team. David Brewer comes to Mydex from the Royal Mail's subsidiary iRed Partnership where he was CIO. He will focus on Mydex' public sector business development. At iRed Partnership David led planning and development of the Royal Mail's digital letter box and other services to help organizations with digital channel shift. He brings a deep understanding and passion for the practicalities and implications of personal control over personal data and ID assurance to Mydex."

Mydex is a UK-based personal data store allows people to control their set of personal data. If a user intends to do business with a website, they can connect their data to it and only share it with that particular website.

Personal's principles regarding how the data stores operate are these:

- your personal details are yours. They sit on your side, in your database
- you can use the same data quickly and easily, again and again. The principle is 'input once, use many times'
- the data you store – and how you share it – is always encrypted, safe and secure. Only you can see your data. Other people only see the data you want to share with them.

http://mydex.org/2012/02/21/david-brewer-diana-jeater-join-mydex/

Resources

ENISA (European Network and Information Security Agency) Study on Monetizing Privacy

Economic Study on Monetizing Privacy

"Do some individuals value their privacy enough to pay a mark-up to an online service provider who protects their information better? How is this related to personalisation of services? This study analyses the monetisation of privacy. 'Monetising privacy' refers to a consumer's decision of disclosure or non-disclosure of personal data in relation to a purchase transaction. The main goal of this report is to enable a better understanding of the interaction of personalisation, privacy concerns and competition between online service providers. Consumers benefit from personalisation of products on the one hand, but might be locked in to services on the other. Moreover, personalisation also bears a privacy risk, i.e. that data may be compromised once disclosed to a service provider. Privacy is a human right; thinking about the economics of privacy does not change this basic fact. The authors of this report consider an economic analysis of privacy as complementary to the legal analysis as it improves our understanding of human decision-making with respect to personal data."

http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy

Cost: Free

University of Queensland (Australia) Study

Australians Uneasy with Targeted Advertisements

This study by the University of Queensland, reported on by Google Exposed, reveals some interesting information on the nature of user's expectations of privacy in the Australian Market.

Link to University of Queensland:

http://www.uq.edu.au/news/?article=24504

Video of the Month:

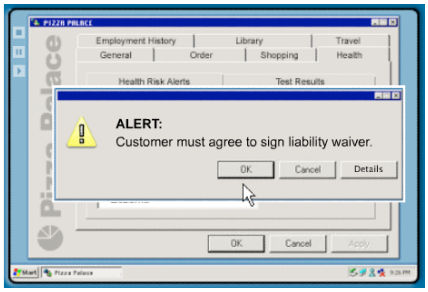
ACLU Pizza Movie

[Yes... that's right. -Ed.]

http://www.aclu.org/ordering-pizza

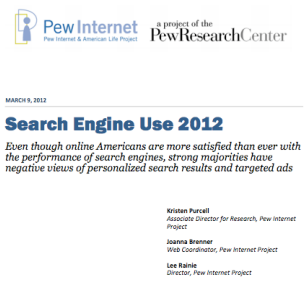
I (Kaliya) highly recommend this video one of the best short pieces that explains the distoepian future we are working hard to avoid with our work in user-centric digital identity.

It is a phone call of a person who is ordering a Pizza, it starts off well but then gets creepier and creepier. The order is placed to a call center and the order taker starts to know more and more about the customer calling..various systems intervene along the way. If I told you more I would ruin the The Video of the Month: ACLU Pizza Movie...so go watch it.



Pew Research

Search Engine Use 2012



"Search engines remain popular—and users are more satisfied than ever with the quality of search results—but many are anxious about the collection of personal information by search engines and other websites and say they do not like the idea of personalized search results or targeted advertising.

Though they generally do not support targeted search or ads, these users report very positive outcomes when it comes to the quality of information search provides, and more positive than negative experiences using search." From the Pew Report Study Web Page.

http://pewinternet.org/Reports/2012/Search-Engine-Use-2012.aspx

Hyperconnected Lives Study

"Teens and young adults brought up from childhood with a continuous connection to each other and to information will be nimble, quick-acting multitaskers who count on the Internet as their external brain and who approach problems in a different way from their elders, according to a new survey of technology experts.

Many of the experts surveyed by Elon University's Imagining the Internet Center and the Pew Internet Project said the effects of hyperconnectivity and the always-on lifestyles of young people will be mostly positive between now and 2020. But the experts in this survey also predicted this generation will exhibit a thirst for instant gratification and quick fixes, a loss of patience, and a lack of deep-thinking ability due to what one referred to as 'fast-twitch wiring.'"

http://pewinternet.org/Reports/2012/Hyperconnected-lives.aspx

Cost: Free

Here's a Great Series of Blog Posts on Big Data by Alan Mitchell

Big Data = Big Dead End? Or Big Data = Big Impact?

Alan Mitchell's Great Series of Blog Posts on Big Data. While there's too much here to arrange any meaningful summary, here's a snippet:

> "But if we look at the really big value gap faced by society nowadays, it's not the ability to crunch together vast amounts of data, but quite the opposite. It's the challenge of information logistics: of how to get exactly the right information to, and from, the right people in the right formats at the right time.
>
> "No matter how big, exciting and impressive Big Data is, that's one thing it cannot do because it is dealing with statistics, not specifics. Instead, all it really offers is more of the same: more data collection by the same entities leading to more data crunching. While the volumes of data now being generated may be unprecedented, Big Data is actually just a continuation of a very old trend, not something new."

http://www.mycustomer.com/topic/customer-intelligence/big-data-big-crm-opportunity-or-big-disappointment/136742

Special Report

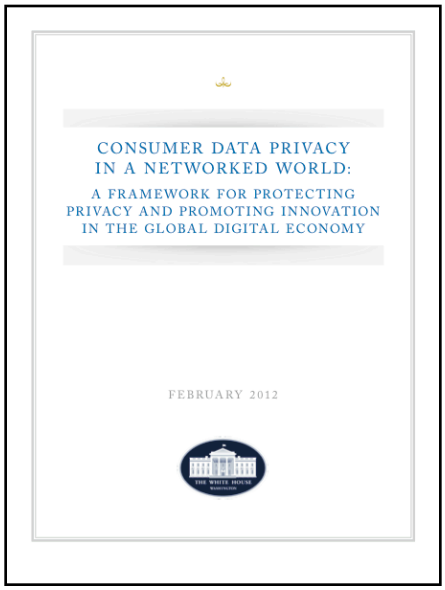
Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy

PDF: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

February 23rd the Obama administration released a blueprint for a Privacy Bill of Rights [Post on White House site]

by Kaliya "Identity Woman" Hamlin

The title of the report gets to the heart of the issue by naming the specific type of privacy that needs to be addressed as "data privacy." It also highlights the realm within which data collection is happening and affecting people most today in their role as citizens who happen to buy things every so often making them consumers.



The report opens with a cover letter signed by President Obama and the opening line of his comments get to the heart of the issue:

> *Trust is essential to maintaining the social and economic benefits that network technologies bring to the United States and the rest of the World.*

The next paragraph continues:

> *Privacy protections are critical to maintaining consumer trust in networked technologies. When consumers provide information about themselves...they reasonably expect companies to use this information in ways that are consistent with the surrounding context.*

(Note that this use of the word trust is an emotive feeling experienced by people in the system overall, not any particular one of the technologies that make it up.)

The fact that respecting context within which data is collected is named in its own right is the most notable new emphasis, compared to prior government privacy guidelines, This bodes well for the personal data ecosystem approach that puts the person at the center of their own data lives giving them tools to share relevant information about themselves in relevant contexts.

It articulates that companies who touch people's data need to behave going forward and encourages a change in business practices.

Consumer-facing companies need to act as stewards of personal data that they and their business partners collect from consumers.

Companies that collect data without direct consumer interactions or a reasonably detectable presence in consumer facing activities should seek innovative ways to provide consumers with effective individual control. Consumers should always have a way of withdrawing consent, however: data that cannot be reasonably associated with an individual is not subject to the right and withdrawal of consent.

The White House is supportive of legislation that adopts the principles of the Consumer Privacy Bill of Rights, and even without legislation they will convene multi-stakeholder processes that use these rights as a template for codes of conduct that are enforceable by the Federal Trade Commission. They highlight that the principles outlined provide a consumer data privacy framework that is interoperable with international partners.

The administration outlines the fact that the government has a role in convening discussions amongst stakeholders which it outlines as:

- Companies
- Privacy & Consumer Advocates
- International Partners
- State Attorney Generals
- Federal, Criminal, and Civil Law Enforcement
- Academics

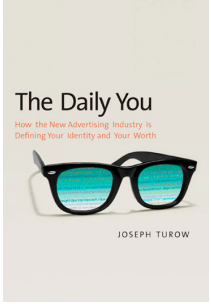
What is not clear is what they mean by an open transparent multi-stakeholder process - which is what they call for. The current methods outlined by the NSTIC program office at NIST for NSTIC have not earned industry confidence and my contacts in the dialogue and deliberation community are disillusioned with the Obama administration's open government meetings and rhetoric that is not creating new open process.

I always check out the footnotes to see what sources are being tapped and to learn if there are new sources that I had not known about before. I found a great one in this report - PRIVACY AND THE NII [National Information Infrastructure]:Safeguarding Telecommunications-Related Personal Information published in 1985 by the National Telecom's Information Administration's (http://ntia.doc.gov/legacy/ntiahome/privwhitepaper.html). It is worth looking at just because it gives a sense of where the language we had to talk about the issues we are discussing now was 30 years ago.

Skip to Appendix A for an outline of the full text of their proposed Consumer Privacy Bill of Rights which applies to personal data, which means any data, including aggregations of data, which is linkable to a specific individual. Finally, Appendix B does an amazing job of articulating the data privacy rights that are put forward in the document relative to OECD Privacy Guidelines (excerpts), DHS Privacy Policy (generalized) and APEC Principles (excerpts).

Book Review

The Daily You: How the Advertising Industry is Defining Your Identity and Your Worth



by Joseph Turow

March 2012

Review by Kaliya Hamlin

http://yalepress.yale.edu/book.asp?isbn=9780300165012

Author Interview on Fresh Air: National Public Radio(US)

The introduction begins by contrasting the story about the power consumers have as the captains of their own media ships and the emerging system of profiling and reputation-making, which is fomenting a prejudicial force that enables new forms of social discrimination.

He opens his thesis by articulating what was true at the beginning of the commercial web that the commercial potential for marketers to profile people was hidden from public view and he argues basically remains true today. The book does an excellent job of tracing the history from the first days of the commercial web and describing what has unfolded with online advertising between 1994 and 2011 a kind of "spanish civil war".

The 2nd chapter is well researched and does a through job of explaining how we go there and some key developments that got us to the state of online tracking and surveillance we have today.

Examples:

- The creator of the cookie rejected the idea of creating a single identification number that a person's browser would use in all web explorations.
- In 1996-1997as the first ad-networks were appearing that used cookies the the IETF identified cookies as a privacy threat
- Tracing the history of COPPA (the Children's Online Privacy Protection Act written about in issue #2 by Denise Tayloe) to a Center for Media Education report called Web of Deception [excerpts I found on Archive.org] lead to hearings in the US Congress and the passage of COPPA.

Chapter 3 focus is a survey of the last decade and how things have evolved more recently including the rise of Google.

The next chapters call attention to contemporary industry practices including seeing consumers - visitors to websites, citizens engaging in our democracy as either Targets or Waste - that is those viable and relevant to be targeted because there is enough information about them to personalize ads...and target them and those who are waste...not enough is know about them...to effectively target them with high paying adds so they are a waste of time. The reason for this is that "advertisers are looking for what they call "scale", the ability to purchase huge numbers of individuals who fit their targeting needs without the expense and chore of having to cherry pick them across thousands of web publishers"

He says that publishers today feel trapped at the bottom of the food chain because they just host content. Ad-Networks run ads alongside publisher content but the real winners are Data Exchange firms because they have the data about the web-surfers, viewers, consumers and because they know more about the people coming to the sites they have more data about them. They are as he says "naturally stimulated" towards "unprecedented data-collecting activity towards individual" the kinds of data points they are seeking include:

- social background
- location
- activities
- social relations

In research survey's 78% of American adults do not realize that having a "Privacy Policy" is merely an invitation to read how some companies treat their information. He points to other research survey's as well for example 79% of 1,500 adults participating in a nationally representative survey agreed with the statement "I am nervous about websites having information about me." He notes that data firms are working to link off-line data to email addresses and personal facts that people reveal on the social web.

He mentions many companies in the book (a list is at the end of this review) but he calls out one company in particular RapLeaf (I wrote about them on my blog many years ago). Without consumer awareness or consent, the company collects e-mail addresses via various means and profile people via social network scraping. They have 900+ million records of 400+ million consumers including 52+ billion friend connections.

Beyond just talking about what is happening with the advertising, publishing and all the new company segments emerging...he focuses on the ethical and social implications of what is happening. The content of news sites is being shaped or customized not by consumers themselves by by their social profiles.

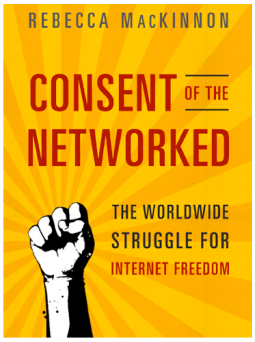
He concludes with this:

People's awareness of differences tin the content they receive may also create or reinforce a sense of distrust about the power of organizations over which they have to control to define and the position them in the social world.... How do we make sure that people with power over our digital lives will not abuse that power?

Companies named in the book: BlueKai, RapLeaf, Invidi, eXelate, NextJump, The Daily Me, Neilson's, ComScore, RevTrax, Media6Degress, Mindset Marketing, Medicx Media Solutions, Experian, Equifax, Trans Union, Reed Esevier, Axciom, BlueKava, Ring Leader Digital, Lotame, Zenith Optimedia, Associated Content, Demand Media, Answers.com, ShopRight, Catalina, Invidi, Visible World, Combe Interactive Comunciation, Teracent, GroupM, 24.7 REal Media, Tacoda, Bridge Track, Teracent, NextNewNetwork.

Consent of the Networked:

The Worldwide Struggle for Internet Freedom



by Rebecca MacKinnon
Review by Kaliya Hamlin

Book Website:
http://consentofthenetworked.com/

Rebecca's TED Talk:
http://www.ted.com/talks/rebecca_mackinnon_let_s_take_back_the_internet.html

The book addresses the urgent question of how digital technology can be structured, governed and used to maximize the good it can do in the world and minimize evil.

It sounds like it might be simple but the constraints on freedom in the networked world are different then past struggles for social freedom and democracy *"now that corporations and governments that build operate and govern cyberspace are not being held sufficiently accountable for their exercise of power over the lives and identities of people who use digital networks. "*

MacKinnon received a fellowship to write the book and did impressive research that touches on the work of many other authors. As an aside, in reading the book I was glad she referenced my articulation of the privacy issues surrounding Facebook's choice to out (make public) social graphs and the groups you follow. She also mention's Doc's VRM.

She worries that if those who are networked...do not consent to how the network systems are governed, we will end up with Networked Authoritarianism, like a DictatorBook. There is a chapter called Facebookistan and Googledom within which she articulates the core issue - that a new private sovereignty exists where we must live under the ever changing Terms of Use that we must consent to or not use their services. She points out that there is no clear model for constraining the power of big data companies.

MacKinnon highlights that there are two main modalities on the network world wide the internet and the phone network. Mobile devices are a major avenue of engagement on network systems and have played a critical role in democratic organizing in places like Egypt. However anyone with access to a phone service provider can easily identify a phone number and unique hardware. She digs deeper in the chapter about social networks and the large online service providers asking if they are the new digital sovereigns:

They control who knows what about our identities under what circumstances; our access to information publicly and privately and even whom and what we know. The companies controlling our digital networks and platforms represent pivotal points of control over our relationships with the rest of society and government. Without transparency and accountability in the use of this information, democracies will be eroded.

She highlights that the designers of online social networks that are being used world wide are being designed by those with these qualities:

- sheltered
- affluent
- Americans

and without genuine:

- social
- political
- religious
- or Sexual vulnerability

She generalizes correctly in my opinion that they generally hold the belief that all people should be transparent and public re: online identity and social relationships.

Facebook sees itself as an innovator "helping people manage their identities and reputations online, in contrast to the lack of control that exists on the internet as a whole." while at the same time making statements that those who have different identities in different contexts of their lives are not people of integrity.

She makes an interesting analogy talking about how and why we developed civilizations in the world to organize human society and systems....she argues that it it is now up to world's netizens (not governments) to figure out how to build a sustainable civilization within the new digital rainforest.

The internet freedom movement she says has not even arrived at the same point of global public awareness that the environmental movement achieved by the first Earth Day in 1970. However, she envisions the mergence of a dynamic coalition on the internet rights and principles.

I will conclude by sharing this quote that gets to the heart of her book and also makes the point that those of us working on developing a personal Data Ecosystem should do so quickly and well so that business and people create it in ways that are mutually beneficial and we don't leave it to be shaped by government regulation that could distort it.

If enough people feel they cannot trust internet and telecom companies to be honest about what data is gathered about users and customers with whom and how it is shared and why the companies cannot reasonably expect to not be regulated with increasing aggressiveness.

Opinion

Personal Data as a New Asset Class: Petroleum or Snake Oil?

By Sara Wedeman

In the World Economic Forum's January 2012 report, Personal Data: The Emergence of a New Asset Class, Meglena Kuneva, European Consumer Commissioner, was quoted saying:

Personal data is the new oil of the Internet and the new currency of the digital world.

According to the study's authors, personal data are "generating a new wave of opportunity and societal value creation." Using "medical records, employment data, bank accounts, tweets, texts, emails, phone calls, geographic coordinates and search profiles," writes the author, "Firms collect and use this data to support individualized service-delivery business models that can be monetized."

Although the report concludes, laudably, by pointing out the importance of owning one's own data and making one's own decisions about how it may be used, I'd like to highlight some concerns that give me pause. As many of you know, personal data and privacy are incredibly complex issues; more so than can be addressed in a year of op-ed pieces like this one. Yet as a behavioral economist with over 20 years' experience studying human behavior, I see a number of obstacles - methodological, social, and procedural - to which we need to attend.

For me, the first red flag is the reference to medical and credit data. Data violability and accuracy problems predate the Internet. Insurance companies have long used something called the Medical Information Bureau (MIB), a private database for insurers that captures highly sensitive information medical information about those applying for insurance. It has been heavily criticized for privacy and accuracy violations Credit reports are notoriously inaccurate. My own credit record is a case example. It has, since 1988, listed me as the owner of a condo in Salt Lake City – a town in which I have never set foot. My repeated efforts to force credit reporting agencies to correct the error have simply disappeared into the great void.

My next concern relates to the parallel drawn between oil and personal data. To be fair, Ms. Kuneva may simply be suggesting that personal data lubricates commerce, just as oil lubricates a car's motor. Yet, the analogy itself is intellectually misleading. Since oil is convertible into cash at a price established by the market, her comment seems to imply that personal data could or should be bought, sold, and traded freely, as is petroleum. Although I believe deeply in the personal and economic value of connectivity, this notion disturbs me. My reaction: the line "Fools rush in where angels fear to tread." is clearly an enduring truth for the ages. The premise that data is a form of currency does not hold water. It fails because it ignores the essence of we know about how, and how not to perform research on human subjects.

At a very basic level, to view them as equivalent – or even comparable - is to make a substantial break with reality. Oil is not 'alive'. Those long-dead plants and animals have no reputations to preserve and what they did or did not feel at any particular point in time is quite unlikely to come back to haunt them. Other than responding to temperature change or choice of refining method, oil does not "behave" differently in different social contexts.

People are sentient beings in an unending process of becoming. As the report observes, there is presently no universal set of standards to protect us from complete strangers drawing peculiar conclusions about us in pursuit of their own purposes. For instance, tracking back to the source URL for a visitor to my blog, I learned that I had been classified in the marketer's report as a "Gen X" male. How the analyst got from my mentioning that I like chili lime taco chips and grapefruit soda for breakfast to tagging my age and gender (both, incorrectly) is a mystery to me. Acknowledging that the cat is already out of the bag, the report's author urges us to get busy constructing socio-tech protocols that are user-centric and trustworthy. I concur.

My next concern: human identity is fluid and situational, changing constantly with time and with experience. Psychologists have demonstrated that the individual is the wrong unit of analysis. Intangible social forces in one's immediate context heavily influence most behavior. If anything, the social environment may be more influential than that which lies between any one person's ears. In The Sociocultural Turn in Psychology: The Contextual Emergence of Mind and Self, authors Kirschner and Martin describe how this works.

The sociocultural turn in psychology treats psychological subjects, such as the mind and the self, as processes that are

constituted, or "made up," within specific social and cultural practices. In other words, though one's distinct psychology is anchored by an embodied, biological existence, sociocultural interactions are integral to the evolution of the person.

In short, while oil is a thing, people – and their identities – are not. Massive increases in computing power have enabled us to analyze data at a level never before possible but this in no way implies that the results will be valid, reliable, or meaningful. To treat shot-in-time personal data as a stable object is to distort reality beyond recognition. I get the sense from my conversations with PDEC that WEF understands this in a general way and that's a relief.

We have here established that personal data circulating out on the 'net is not analogous to currency and that it cannot be disconnected from the living person without degrading accuracy. To do so is to commit the logical fallacy of reification, treating an abstraction as if it were a concrete event or physical entity. Sometimes the practice is ignorant but otherwise benign. However, in the era of 'big data,' the potential for harm is tremendous. To separate an individual from his or her data and to attribute meaning thereto, without neither their knowledge nor consent, is a basic violation of human rights, morally, ethically, and financially.

Your data are yours and yours alone. Once they leave your possession, what will be done with them, by whom, to what ends, is anybody's guess. That's why I'm somewhat relieved that these issues are front and center at WEF.

Some people still believe that photographs steal one's soul in that they capture and reify something ephemeral. With big data, that old superstition has the potential to morph from superstition to reality. It is simply too important to leave to others. If people are really going to survive this transition, they are going to have to start caring dramatically for "their data" and its uses. Care, caution, and collective attention to these issues are everyone's duty. In another piece, I'll talk about how the behavioral economics concepts of framing and setting pro-social default parameters can help. In the mean time, educating people about this complex terrain, and teaching them how to take responsibility for protecting their data from use without consent, will be among our gifts to the future. Caveat Emptor.

Opinion

Words of a Feather

by Tony Fish

Ask a group of friends to define any of the following words:- Private, Privacy, Trust, Sharing, Personal data, Rights or Context. Whilst you may start the evening as friends; you may well end the evening questioning integrity or the definition of "Friends." Digital data has become a new politics, religion and sex conversation topic that we should avoid discussing. But why?

My view is that, just like in religion and in politics, we start from different points (knowledge and mood today) with varying expectations (outcomes) and personal experiences. This opinion addresses our different starting points as we get to read about expectations from daily Fear, Uncertainty and Doubt articles that form fabulous news headlines and personal experience that are, well... personal.

No attempt here is made to convert or sway anyone from their own trusted viewpoint. My purpose is to present framework that enables us to converse from our different starting points. These origins are key because they frame both the fact base and the available logic that is appropriate to discuss them.

First Framework: Private is not one State

If I start from an origin of talking about Files (audio, video, images, docs) or Information (content) when thinking about what data are private and which are shared; at the most basic level the files I create on my machine, then they are Private. I am in control of the file and the content is shared with no-one. However if I start from an origin of Communication (voice, text, IM, tweet, blog) and I restrict the communication to one other (trusted) person (one-to-one) then this level of conversation is also Private. But unlike my Files, this private data is now shared.

To add confusion to a working definition of what is "private",we can also declare trusted sharing across files, collaboration, communication and information private as well when we restrict the sharing to one (or in some cases a very small group). This action assumes that we also trust the medium by which we share. The implication of this assumption creates the core of the struggle to define what Private is unless we also provide purpose, context and trust.

Second Framework: Share is not one State

The word Share (sharing, shared, shares), like so many English words has a number of uses (noun and verb) and contexts. Share comes with context and a dependency on the person (trust) to obey the rules/ processes/ methods under which the sharing took place. However, shared quickly encounters the world of value and benefit of the beholder, which leads to breaches and to debates such as "in the public interest" and "the public is interested" in. In the Communication and Collaboration worlds, sharing is a basic requirement and just like file and information, a level of trust is implied. However for collaboration, the trust framework applied can be driven by requirement, skill, and delivery over and above established trust principals. The implication is that Sharing introduces group complexity and levels of trust and policy. "Shared Privately" is different from "Privately Shared."

Third Framework: Public is not one State

So now, let's move to discussing the journey from private to public. Public in communication and information terms is mainly about a one-way conversation (a broadcast) whereas if your centre of gravity is collaboration, Public is about anyone having the ability to add, collect, provide, edit, delete, improve or refine. Starting from a File, Public means access. The implication is that Public introduces contentions between the dogma of broadcast, access to, and crowd source.

Given that it is difficult to agree how to use the terms Public, Private, Trust, and Share within our conversation, I am not surprised that we are culturally wrestling with Personal Data, which may be a subset of the information/knowledge column or its own unique new column as it needs some better defining of what the terms, especially privacy, mean….

Tony Fish is the head of AMF Ventures, and the author of My Digital Footprint. He is also a PDE board member.

FEDERALIZATION

(continued from Page 2)

Started in early 2010, the vision of this project is to develop software for small "plug computers", which can be installed at one's home or office to protect privacy and enable free communication. In other words, the idea is that personal data is stored locally on a FreedomBox rather than in the cloud, and that social networking and other communication happen directly from one FreedomBox to the other rather than via an intermediary service provider. Privacy, independence, data portability and fine-grained access control over who can access your personal data are obviously core goals of the project.

On the technological side, at this time the FreedomBox is mostly a collection of ideas and software packages rather than a concrete product. It can be installed on various plug computers such as the GuruPlug, SheevaPlug or DreamPlug by GlobalScale, most of which are based on ARM RISC processors. Open hardware projects like Raspberry Pi are also starting to become relevant, and might eventually become the platform of choice for FreedomBox.

It is a Debian-based Linux system and attempts to mostly use, customize, and bundle software that already exists, rather than developing everything from scratch. Much work is currently also put into the design and implementation of a user interface that makes the FreedomBox easy to access for everyone. Debian was chosen for its proven software distribution mechanisms that should be reliable even under adverse circumstances, and for the social guarantees around freedom that are commonly associated with Debian.

It is obvious that the limited hardware characteristics of plug computers also put restrictions on the kinds of software that can be run on a FreedomBox. Despite this, the FreedomBox is a general purpose platform which is perfectly capable of providing HTTP, FTP, SMTP, SSH, DNS, or DHCP services, as

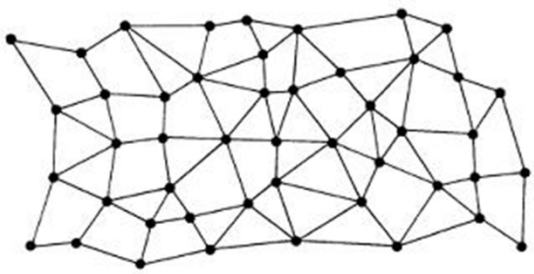
well as executing PHP, a JVM, a MySQL database server, or a BitTorrent node. Applications on the FreedomBox will cover pretty much all social networking needs, e.g. e-mail, web browsing, publishing, and file sharing. The protocol of choice for many of these applications will be Jabber/XMPP, which can be used for sending text, audio and other media, as well as structured data. It is likely that a modified version of the Prosody software will be used.

One of the paramount goals of the FreedomBox is security. A FreedomBox is designed to have one owner (with

administrative privileges) and multiple users, each one of which has an associated GnuPG key pair for authentication and encryption purposes. The goal is to encrypt all communication, and to employ a social key management technique for key recovery, which means that your private key is split into parts which are then distributed among a set of trusted friends. No single friend can impersonate you, but in the event you lose your key, it can be re-assembled if all your trusted friends collaborate with you. In fact, not only your key, but also backups of your personal data can be distributed among your friends, so that even in the event of a complete loss of your FreedomBox, you can re-populate a new one with all your data. The notion of who your friends are will be built into the FreedomBox on a very low level, because some of the core functionality such as key management rely on it. For optimal security, encryption of the entire file system is also a goal, although there are several challenges to be solved to achieve this.

Another innovative security detail of the FreedomBox (in alignment with the spirit of moving away from centralized structures) is related to trust. Instead of relying on traditional SSL certificate issuing authorities which today are built into all browsers, the FreedomBox will instead use decentralized technologies such as MonkeySphere, in order to replace the traditional SSL trust model with a PGP-based web of trust. This approach to encryption and trust is intended to be used both for browsing and for message passing, which in practice means that a FreedomBox will trust another FreedomBox based on prior interactions between their users, rather than based on signatures by central authorities. Key management happens mostly behind the scenes, and its associated complexity is hidden from users.

Regarding the networking capabilities of the FreedomBox, it can connect to an existing wireless network, or act as a router. Making the FreedomBox work with mesh networking protocols is also on the agenda, as is using Bluetooth to make it communicate securely with mobile devices. Besides being a device for data storage and distributed communication, the FreedomBox can also serve as a classic gateway between a private network and the outside world, meaning that it can act as a firewall, scan for viruses and irregular communication patterns, run software such as Privoxy to remove cookies and other tracking technologies, etc. And it can be used for SSH port forwarding and tunneling, as well as run the Tor onion-routing software, meaning it can relay, disguise and anonymize traffic that passes through it.



Decentralized Network Architectures

The Political Perspective

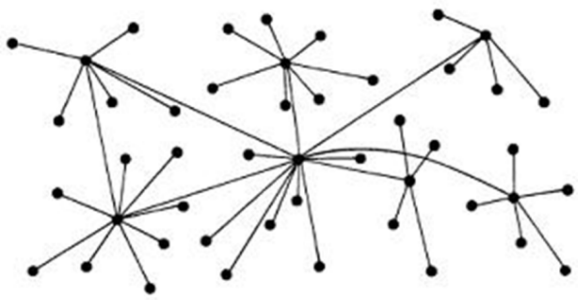
When discussing decentralized architectures, it becomes clear that their respective advantages and disadvantages cannot be evaluated purely based on technological properties. Instead, there are usually also ideological questions and challenges involved, such as finding the right balance between freedom and security that is healthy for a democratic society. A fascination with certain decentralized approaches may therefore be (partially) explained by a social desire to reduce the influence of traditional political and economic authorities.

This political character is most visible when technology projects that try to implement decentralized communication patterns are driven by political movements which themselves are characterized by decentralized organization. For example, this is the case with the GlobalSquare project, which is inspired by the Occupy Movements and makes a clear political statement by claiming that democracies just like the Internet today have incorporated too much centralization.

Another perspective is that of human rights. While there are different opinions on whether Internet access and privacy online actually constitute human rights themselves, or whether they are merely instruments that have the potential to enable human rights, it is the decentralization of online systems that appear to strengthen this potential. For example, Professor Eben Moglen of Columbia University argues that the 4th Amendment of the U.S. Constitution implies a technology architecture that is not "in the cloud" but rather within our homes, where an individual's protections against unreasonable search and seizure are strongest.

Political, financial and academic resources are more and more being devoted to such efforts, for example by the New America Foundation, which supports projects to build technology for a distributed, open-source telecommunications system, by MIT's Center for Civic Media, which researches and invents "new technologies that support and foster civic media and political action",

by the European Commission's No Disconnect Strategy, by the University of Toronto's Citizen Lab, by Stanford's Program on Liberation Technology, or by the Harvard Berkman Center for Internet & Society's Internet & Democracy project, an initiative with an explicit focus on the Middle East.Drawbacks



A Distributed Network Design

Despite advantages of decentralization, many projects that have tried to implement their functionality in a decentralized way have failed, and as a consequence have either reduced the degree of decentralization in their design, or have switched completely to a classic centralized architecture. One of the most spectacular examples is the Internet TV service Joost (a.k.a. "The Venice Project"), which in 2007 started with highly innovative peer-to-peer video streaming directly between client computers, but eventually switched to a Flash-based web player. Another example is OpenID, which in 2005 started with the utopian vision of a completely decentralized identity layer for the Internet, but eventually ended up mostly as a mechanism for supporting a very homogeneous ecosystem of only a few major Identity Providers (IdPs).

A recent paper titled "A Critical Look at Decentralized Personal Data Architectures", which mentions several PDEC members, tries to identify reasons why decentralized architectures – despite their advantages – are having such a hard time to gain adoption in the fields of Personal Data Stores, Vendor Relationship Management, and social networking. It argues that privacy, utility, cost and innovation are four important factors that hard to address properly in a single architecture. As concrete problems with decentralized architectures, the paper lists among others:

- The fact that certain operations such as search, trend analytics, or fraud and spam detection are difficult to achieve without a unified view on the entire system.
- The difficulty of agreeing on standards and achieving technical interoperability, which is easier if only a single entity is in charge of operating a system.
- The reduced speed associated with the higher administrative overhead of a decentralized system, such as synchronizing clocks and minimizing data duplication.
- The higher costs for developing, hosting and maintaining the overall system.
- Difficulties for the user, e.g. the need to install client software, or the challenge to understand the nature and advantages of a decentralized system.

As recommendations, the paper advises to consider the economic feasibility of a design, to honestly evaluate what features and benefits users really want, to offer advantages other than just privacy to users, to address not only the

What Do we Mean When we Say "Peer-to-Peer"?

The term "peer-to-peer" (P2P) has originally gained much popularity in the context of file-sharing systems and is now again on the rise. However, when we say that something happens "peer-to-peer", then that can mean different things, depending on what layer of a communications system we are talking about. The following list describes the different meanings of "peer-to-peer" that are commonly used and sometimes confused:

P2P only in the social sense, i.e. exchange of information happens between two individuals, but via a centralized technical infrastructure. Examples: Facebook, Twitter.

P2P in the sense that the technical infrastructure does not rely on any single centralized component, but it still distinguishes between clients and servers, i.e. individuals choose which server they want to use. This is called federation. Examples: E-Mail, Federated Social Web, OpenID.

Fully distributed P2P on the network layer, i.e. either there is no distinction between clients and servers, or each participant effectively operates their own server. Examples: BitTorrent, FreedomBox.

Fully distributed P2P on the physical layer. Examples: Mesh networks such as Freifunk or Funkfeuer. - Markus

technological side but also incorporate socio-legal approaches, to design with standardization in mind, to target limited feature sets for a minimum viable product rather than trying to boil the ocean, and to work with regulators to help achieve a balanced environment.

Decentralized Network Architectures and the PDE

So what do recent initiatives for decentralization mean for the emerging PDE? Because of their properties of giving individuals more control over their personal data and communication, they are clearly relevant. The FreedomBox for example could essentially become your Personal Data Store (Service, Vault, Locker, …), which is truly under your control rather than in the cloud, and guarantees your privacy. Other goals of the PDE such as making your personal data discoverable, or creating business models around personal data, do not yet appear to be part of the FreedomBox vision, but can possibly be achieved with the help of brokers as intermediary service providers, sophisticated peer-to-peer routing mechanisms, and the PGP web of trust component. In any case, the failure or success of the FreedomBox project is likely to greatly affect the nature of the PDE.

Within PDEC, architectural forms of different initiatives already vary greatly, and they exhibit different advantages and disadvantages. Several companies within and outside of PDEC are working on personal data related solution that exhibit certain degrees of decentralization, for example:

The apps ShareShelf and WannaBet? by Tangled Web Communications consider mobile devices “part of the cloud” and do not require any storage of personal data outside of the device. Some initiatives such as the TAS3 or the Connect.Me “Respect Network” envision decentralized architectures where multiple service providers can interact with each other without the need for a single centralized component. Singly’s Locker Project contains a component called TeleHash, which connects different instances of the Personal Data Locker to each other, for the purpose of exchanging JSON data in a completely decentralized manner.

Conclusions

The trend toward decentralized systems cannot be ignored and should be incorporated into the vision of a future PDE. In this vision, decentralization should not be understood as a threat to existing structures and entities, but rather as a new asset for both improving privacy and generating new business opportunities. Large enterprises, innovative start-ups and individuals can all be part of this vision and harness the potential of new and decentralized flows of personal data.

One of the main guiding principles should always remain the development of services and products that people are really interested in using, and to make them easy to understand and use. Only very few people will use a system whose advantages are not obvious. Unfortunately, there is often a trade-off between different desirable goals such as privacy and ease-of-use, and most people will choose the latter. Or as James Vasile of the FreedomBox Foundation puts it, “give me convenience or give me death”.

Perhaps for the PDE, the solution will be to find the right balance, i.e. to develop hybrid models that combine the respective advantages of centralized and decentralized structures. A future communications system that relies on a radical peer-to-peer infrastructure all the way down to the physical layer might have many problems, just like highly centralized systems today have many problems.

SO...I just adjusted the pages UP in the document...and you can keep the IMages linked INLINE until the very last moment....but I just shifted things and then these images are “floating” in the document and I have no idea what text they go with...this is the problem.. I “get” They look better floating in teh middle of the page and indeed they should do that in the FINAL verion but I propose that teh “setting of the pictures” be the ultimate last thing that is done so that we can edit and not mess everything up.

A Casual Conversation...

The other day I went out to have dinner at a Pizzeria in Vienna, Austria and coincidentally overheard a conversation at the next table. A group of people was emotionally engaged in a conversation about the collection and mining of personal data online, especially by Facebook. They made it very clear that they were not happy with all their digital identity being controlled by a SIlicon Valley company, and they agreed that something had to change. I thought, yes, awareness about personal data online is now hitting the mainstream. The time for a new PDE has come. - Markus

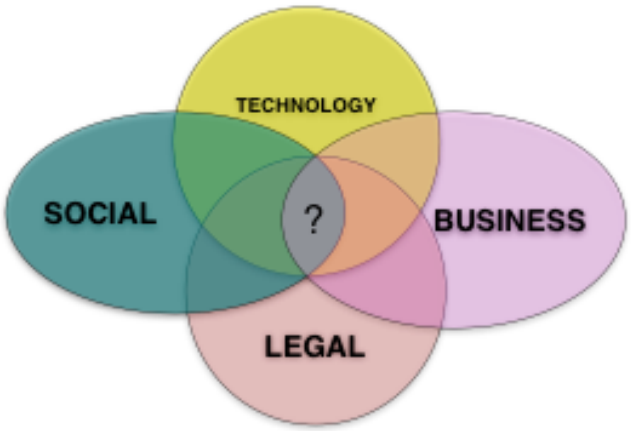
Publisher's Note

by Kaliya "Identity Woman" Hamlin

When ecosystems in nature are working smoothly, things just flow - it seems simple, but there is much underlying complexity.

Our mission is to catalyze a functioning ecosystem with many parties participating, using a diversity of business models based on open standards, with a core underlying tenet being that people have control over their data.

Getting from where we are now to a thriving personal data ecosystem will take time, trial and error, innovative pilots, and collaboration amongst many different companies. However, almost all of the challenges we face getting there fit into four different issue clusters.



The clusters cannot be solved individually or sequentially - we must work to address challenges across all four in parallel.

What are the right technologies? Protocols for systems to talk to each other (one–off hacks, closed standards, or open ones and then at which standards body) the systems themselves (open source, proprietary).

What are the business models that can work? Is there the potential for a diverse ecosystem with many different industries participating and thriving or will one industry "win" or even one "winner take all"? Are there key non-profit-making entities needed at the core of a thriving ecosystem?

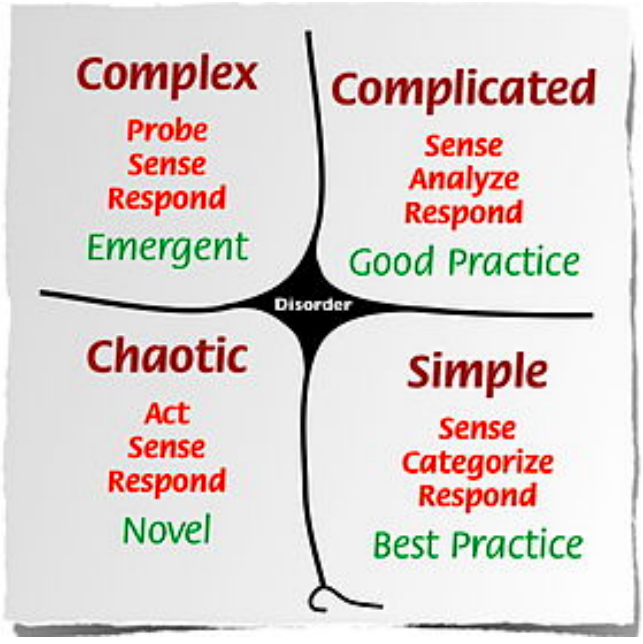
How can the legal issues that come up be addressed? How can large mesh networks of interoperability be brought into being without incurring huge liabilities?

Will people adopt the new innovations? Will people accept or even understand new models of how their data is being handled and used? Will new social norms emerge? What are the user experiences and how can they work for diverse types of people?

It is essential that we not address just one cluster of issues, but support the information sharing and consideration of developments in all of these clusters simultaneously to move the whole industry forward. This is why we cover such a broad range of topics here in the Personal Data Journal, because the challenges can not be addressed in isolation.

I am regularly in conversations with industry leaders who are asking about one small thing they can do, or what is the simple way. It just isn't simple to get all these different issues "solved."

However, we are lucky to live at a time when new insights and models have been develop to both conceptually understand and mathematically model these types of systems. One of my favorite thinkers on such topics is David Snowden who developed the Cynefin (pronounced - Kin evin) framework drawing on complex adaptive systems theory understand different types of problems, situations and systems along with solutions that may apply.



The overall personal data ecosystem system that we are working with is emergent although some aspects are just complicated.

Reports will be for global leaders with "simple" calls to action. However, in the end it will take dedicated leadership across new business ecosystems to build new infrastructure, test out new models, deploy existing standards in innovative new ways, and lead the development of new ones needed for interoperable competitive markets.

The path between here and and a working ecosystem with a whole new set of tools for people/citizens to collect and manage their own data is complex. It is quite evident in this diagram which Ctrl-Shift, a PDEC strategic partner, developed to articulate the range of topics to be covered as part of its Explorer Club in the coming years.

Editorial

EU Privacy and the US Consumer Bill of Rights: A Tale of Two Cities

by Kelly Mackin

With the onward push towards a global society enabled by the Internet, it makes sense that governmental bodies are working to "come to grips" with the digital world regarding methods to protect their citizens from ill-advised, unfair, or predatory data practices. The White House, the National Institute for Standards and Technology, and other centers of power have recently been working to develop consumer protection safeguards while attempting to avoid inhibiting the capacity of digital systems to change and grow rapidly. In related news, in November 2011 (and as reported in PDJ), the European Union announced their first major upgrade to the rules they first established in 1994-1995.

In this piece we will explore the Consumer Privacy Bill of Rights from the perspective of the Personal Data Ecosystem model. At the same time we will compare the European approach with the White House Paper and US approach.

It's not a secret that the Internet is "converging" and obsoleting national legal structures due to its ability to support free flow of instantaneous information across systems, borders and continents. At first glance into this issue this author was expecting to find that the EU and US proposals would be closely aligned to bring the US into closer conformity with the EU and other compliance systems such as APEC. And indeed the Consumer Bill of Rights (CBA) does 7bring the US closer to other systems, but how much closer? And how does this compare against the Personal Data Ecosystem Approach?

The White House Initiative

There are a number of interesting differences in the recently published Consumer Bill of Rights released by the White House when compared to the comprehensive regulations of the EU. For one thing, its not a proposed legislation. It's a white paper laying out what the White House believes are the correct areas for a new law to focus.

It should be clear to anyone paying attention that the CBA does attempt to streamline the expectations of consumers and businesses in the use of the data. It proposes a code of conduct process. It creates a level playing field to prevent privacy policies from saying "we are going to steal all your data and sell it." So far, so good.

It attempts to create a framework to forestall actions of US State legislatures forging ahead with their own laws that make it hard for any company, in the US or elsewhere, to avoid running afoul of 51 jurisdictions with their own laws. So far so good.

The paper gets considerably foggier when it turns to the issues of enforcement. It proposes that the FTC be "directly" empowered to investigate allegations of improper activity. At first look, this sounds like a reasonable idea. But the backlog, delays, and federalization inherent in empowering a commission of the federal government and state attorneys general to process complaints seems to create a tougher set of rules with a weaker chance at enforcement. Those are big hammers that in practice can only handle a small portion of the total number of infringements. This method would likely wind up weakening accountability.

Personal Data as an Asset

A potentially bigger problem exists that the proposed framework appears to miss the economic value and relationships inherent in personal data. And it appears to sidestep the issue of who owns personal data. Is it the company? Is it the person? There doesn't seem to be support in the White House framework for the creation of a personal data economy. The CPA paper does not appear to reflect an understanding that personal data is an asset owned by an individual.

> *"Personal chief policy officer and general counsel Joshua Galper explained to me that right now there is no basis in the law to say that my personal data is real property value. It is considered to be "information" by the courts, not property. The devices that carry your data, like smartphones or computers, are considered property, but not the data itself."* - Mark Sullivan, reporting on SXSW for ComputerWorld

Another important difference is that the rules do not apply to civilian federal government agencies like they do in Europe. In the U.S., civilian agencies are prevented from activities like setting cookies on people's machines. Still, the CBA approach doesn't enable the citizen to use the proposed mechanism in support of their ownership of data held by agencies. While the author tried to find all the points of light in the paper, it is in the end a Bill of Rights for the Consumer

The EU Commission's Goals in Privacy

- **Strengthening the Rights of Individuals** so that the collection and use of personal data is limited to the minimum necessary. Individuals should also be clearly informed in a transparent way on how, why, by whom, and for how long their data is collected and used. People should be able to give their informed consent to the processing of their personal data, for example when surfing online, and should have the "right to be forgotten" when their data is no longer needed or they want their data to be deleted.
- **Enhancing the Free Flow of Information in the Single Market Dimension** by reducing the administrative burden on companies and ensuring a true level-playing field. Current differences in implementing EU data protection rules and a lack of clarity about which country's rules apply harm the free flow of personal data within the EU and raise costs.
- **Extending Privacy Safeguards to Police and Criminal Justice Records Systems** so that individuals' personal data is also protected in these areas. Under the Lisbon Treaty, the EU now has the possibility to lay down comprehensive and coherent rules on data protection for all sectors, including police and criminal justice. Naturally, the specificities and needs of these sectors will be taken into account. Under the review, data retained for law enforcement purposes should also be covered by the new legislative framework. The Commission is also reviewing the 2006 Data Retention Directive, under which companies are required to store communication traffic data for a period of between six months and two years.
- **Ensuring High Levels of Protection for Data Transferred Outside of the European Union** by improving and streamlining procedures for international data transfers. The EU should strive for the same levels of protection in cooperation with third countries and promote high standards for data protection at a global level.
- **More Effective Enforcement of Privacy Rules** by strengthening and further harmonizing the role and powers of Data Protection Authorities. Improved cooperation and coordination is also strongly needed to ensure a more consistent application of data protection rules across the Single Market.

Source: Epic.org

that contains no rights. It contains processes and promotes modes of conduct. It contains implicit principles. It contains methods. But it does not contain explicit rights.

Market Failure of a Different Sort

The Obama Administration doesn't see markets as the solution to many problems. So its a good thing that the proposal does include "stakeholder" participation recommendations that enable all affected parties to "have a voice" in the creation of the rules. In practice those models typically result in having the power reside in the halls of the U.S. Government with citizens and businesses placed into a position to have to plead to a government not to enact rules that could very well harm them. Regulated markets are traditionally slow to react and indeed have been shown to inhibit change, or be vulnerable to influence.

> *"Some economists see regulations as problematic not only because they disrupt market processes, but also because they tend only to bring about more regulations.... In practice, regulators very seldom even consider that the problems they detect may actually be the consequence of prior regulation, so the second option is preferred far more often than the first. The new regulation, however, has unintended consequences of its own that bring about this cycle anew. If unchecked, the result over time is regulation so extensive as to amount to a state run economy.-" Wikipedia article on regulated economies*

That the Internet thrives because government stays out of it to a greater degree than other industries is now considered a cornerstone of the digital economy. That said, the lack of legal frameworks that could set a basic set of personal data rights and rules is in the view of this author a significant problem because it has created a "Wild West" atmosphere where sophisticated players dominate personal data to the detriment of individuals.

The paper seems to be devoted more to transactional security and less to the activities of Big Data, although the FTC report which followed takes a closer aim at data aggregation. It's likely that this is no accident. The White House paper only briefly mentions data mining and behavioral mapping, which of course are two of the biggest threats to privacy in an online world.

Compared with Europe

The EU Privacy law's enactment in the 1990's was to an American eye a major event. It was so all encompassing that governments needed opt outs and individuals needed special exceptions so that they could keep address books. That said, there were a number of notable features of the first law. It painted government and private industry with the same brush save law enforcement. It put the consumer first in most instances, and put the burden of compliance on business and government agencies. It streamlined and minimized differences amongst the European nations with respect to data privacy, and in the view of this author has been a qualified success.

The European Union has as a result long been the vanguard with respect to the protection of privacy. It's strong regulatory framework has as a result become a bellwether for government interventions to protect privacy rights. While the approach has brought significant benefits to the consumer in Europe, it also shares a similar weakness to the US approach in that it does not embrace personal data as an asset class with economic value and allow the consumer to participate in this market. Also, it takes a top-down government approach that avoids the opportunity to create an ecosystem that includes private, insurance-style accountability to better address the shortcomings of the regulation.

Last December, the EU announced a long-awaited update to the regulations. The update calls for a series of changes.

The underlying theme of these new regulations for Americans is that Europe is far ahead of the United States and has vastly more experience in administering a data protection framework. One can see "echoes" of the European regulations in the White House paper, and it generally makes sense that one would. However, the general distrust of the private economy is partly misplaced in both the EU and US frameworks.

Let's go back to auto insurance. The states mandate auto insurance in the US for an automobile no matter who might be driving. In the event of a claim, the motorist files a notice with their insurance carrier, and the insurance carriers on both sides of the event cooperate to resolve the situation. It's a well-oiled example of a set of sensible public laws giving rise to an efficient and competitive market mechanism for the settling of claims without resort to a lawsuit. This is the type of accountability model that should be instituted because it enables private entities to resolve claims amongst themselves while preserving the government's interest in prosecuting egregious cases with clear malicious intent.

Personal Data Ecosystem Approach

The PDE ecosystem could in many respects find its expression in a law based upon the White House CPA. In the areas of accountability, access and accuracy, focused collection, transparency, individual control, and respect for context, the White House paper is a good beginning. The missing piece is a certain blindness for the personal data economy. The author hopes that in the coming months that the White House begins to adjust the model so that it includes specific declarations of individual ownership, and a recognition, as the World Economic Forum does, that personal data is an economic asset.

I also hope that the accountability functions are privatized. It would be much better for both the United States and Europe to have a personal data insurance industry addressing claims than an "enforcement model" that relies on civil and criminal law right from the start. It's possible to obtain the benefits and minimize the risks inherent in personal data with a private claim model that only involves the government if there are systemic or egregious abuses that cannot be corrected as a last resort.

Want to play? Get insurance. Just as in an auto-accident, the insurance companies process and investigate the complaint and pay the wronged a settlement. With that, competition, quality of service, quicker time to resolution, and more teeth appear to ensure accountability. A firm doesn't want to comply? Then the insurance bill just keeps getting higher until it makes sense for them to conform. That's perhaps a better system than federalizing enforcement because it uses the teeth of markets that can contain abuse more robustly perhaps than an agency approach alone.

With the recent announcement of the FTC report and the Consumer Privacy Law just introduced in Congress, that the government is serious about passing privacy legislation in the current year. And while its possible to be hopeful that it will be a good law that promotes both individual freedoms and rights and enable the personal data ecosystem to improve and evolve, a close watch will be needed by interested parties to make certain that in the headlong rush to improve privacy, that the patient survives the surgery.