PERSONAL DATA JOURNAL

Issue N°4 May, 2012

# Privacy by Design

***by Markus Sabadello, Technical Analyst***

The idea of an emerging Personal Data Ecosystem (PDE) is based on several different lines of thought. Ultimately the purpose of the PDE is to help us all make sense of the unprecedented amount of online personal data we observe today. It is about creating new business models and economic opportunities based on this personal data, which has been called a new currency, or asset. It will give individuals the means to control how this asset is used. In doing so, an awareness of the importance of privacy will develop on one hand and on the other privacy by design will become one of the key principles of the concrete solutions that ecosystem members are developing. In this article, we will offer a quick introduction to privacy and then move on to describe concrete resources and approaches to Privacy-By-Design, which is the idea of "baking in" privacy up front into the design of software architectures, rather than considering it a secondary or 3rd-party aspect of classic software engineering or deployment.

## What is Privacy?

There is much discussion (and some controversy) about the concept of "privacy" itself, especially about its application in the online world. Today, we can observe that in the general public as well as among thought leaders, there is a growing awareness of the privacy implications in the increasing amounts of personal data are created, collected, stored and disseminated online. This concept is playing a major role as a catalyst for the emerging PDE. The question of how privacy is understood in different cultures and contexts, and at different points in history, has filled many books. Also, there are several other interesting topics that would require too much space to cover here, such as the existence of a right to privacy, or the overlap of privacy with similar concepts such as security or confidentiality. For the purpose of this article,

let us simply assume that privacy online is understood as the ability for individuals to know how their personal data is collected and used, and to exert choice and control over such use.

This understanding is notably different from secrecy, i.e. a condition in which no data is shared at all. It should also be pointed out that an ecosystem following Privacy-By-Design

## Contents

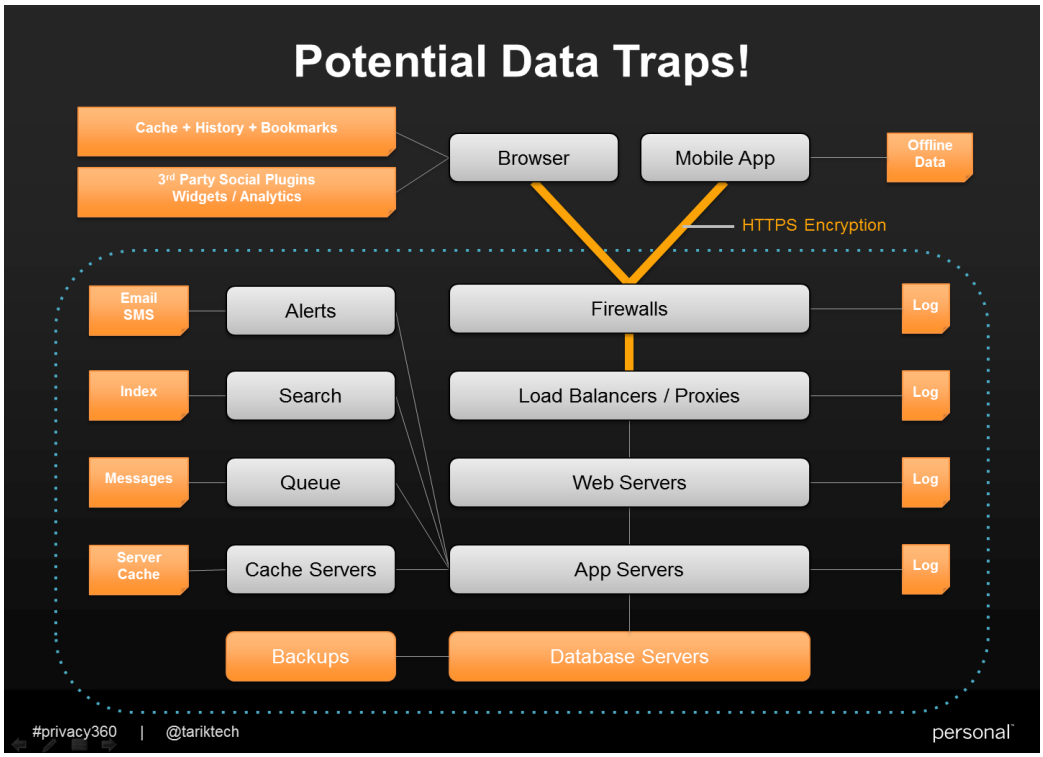
principles will not lead to individuals building fences and completely rejecting the use of their data for social and economic processes. On the contrary, more control will lead to more trust between individuals and companies, to higher quality personal data, to more valuable economic relationships, and as a consequence, to a vast potential for growth and innovation. Therefore, the goal of modern technology in this area should also go beyond basic Do-Not-Track mechanisms, which simply allow individuals to turn off tracking of personal data and behavior, but do not offer ways of specifying in more depth what should be allowed and what should not be allowed in different circumstances.

## Privacy-By-Design

The idea of Privacy-By-Design, according to one definition, "aims at building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles".

Dr. Ann Cavoukian – Ontario's Information and Privacy Commissioner is the leading proponent of Privacy-By-Design – has been working on this concept since the 90s. On her website, she explains that Privacy-By-Design touches on the three areas information technology, business practices, and physical infrastructure. She lists seven foundational principles that should be observed when designing for privacy:

**Proactive/Preventative:** Invest time up front to anticipate potential privacy issues, rather than being reactive. Problems should be prevented before they arise. In a default setting, no action is required for personal data to be automatically protected.




**Embedded in Design:** Privacy-protective measures must be seamlessly integrated into the core functionality of any system or business process, rather than adding them afterwards. Privacy is a concept that becomes an essential component of the functionality delivered, without diminishing it.

**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

**Subscriptions:**
Phil Wolff: phil@pde.cc

Enterprise licenses for The *Journal* are available at http://www.pde.cc/journal. Now you can influence your entire firm.

Individual Subscriptions: $645 suggested Min $150/12 issues.

*Personal Data Journal* is published by the **Personal Data Ecosystem Consortium.**

Executive Director:
Kaliya Hamlin

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

http://personaldataecosystem.org

**Positive-Sum not Zero-Sum:** Designing for privacy does not imply a sacrifice or tradeoff with other goals such as security or functionality. On the contrary, all such legitimate interests can be accommodated in a positive-sum, win-win manner.

**End-to-End Security:** Theft and loss of personal data can be avoided if an organization designs its systems and processes for privacy in advance. Privacy principles then stay active throughout the entire lifecycle of the data (end-to-end). This eliminates the risk of a privacy breach.**Visibility/ Transparency:** In order for individuals to be certain that their privacy is protected, they need to know who has their personal data, and what it is being used for. Both individuals and organizations need to be able to audit and verify technology and business practices.

**Respect for Users:** Privacy is about personal control and freedom of choice. Privacy-By-Design requires organizations to keep the interests of the individual uppermost, and it therefore not only protects, but also empowers.

The following is a non-exhaustive list of general goals as well as concrete measures that can be taken in the design of information technology to implement the above principles:

**Anonymity:** The true identity of an individual or other party of a transaction should only be learned when necessary to complete the transaction.

**Data minimization:** Service providers should store and transmit only the bare minimum of personal data that is needed for any given purpose.

**Anonymization:** If personally identifiable information (PII) is stored or processed by a service provider, it should be anonymized when it is aggregated, analyzed, no longer required, or passed on to third parties.

**Encryption:** Data should be encrypted whenever possible, both when it is stored ("at rest") and when it is transmitted ("in transit").

**Pairwise Pseudonyms:** Pairwise unique pseudonymous identifiers should be used to express relationships between parties, to prevent them from correlating their users' identifiers.

**SSL/TLS:** HTTPS should be used for login, data transmission, and API access, in order to ensure the confidentiality of personal data that is transmitted over the network.

**Multi-tiered Architecture:** MTA should be used with (at least) a clear separation of the storage layer from the business logic layer.

**Data Portability:** DP should be supported, i.e. the ability for users to take their data out of one system and move it to another.

**Data Termination:** A right to be forgotten should be offered, i.e. a way for users to completely delete all their data, history, and account information.

**Reasonable policy defaults:** This can make a significant contribution to the privacy characteristics of a system, since many users will not know or care how to adjust their settings.

**Access Controls:** Careful design of authorization, clearance levels, permissions, obligations, etc. when accessing personal data.

**Anonymous Mode:** Support for "private browsing" / "incognito" modes in software.

**Limited Crumbs:** Limiting the use of web technologies that can have privacy implications, e.g. cookies, referrer headers or fingerprinting.

**Security Best Practices:** Application of security best practices for information storage technology, especially when modern cloud services are used.

**User Notification:** Giving users a way to be notified whenever their personal data is used.

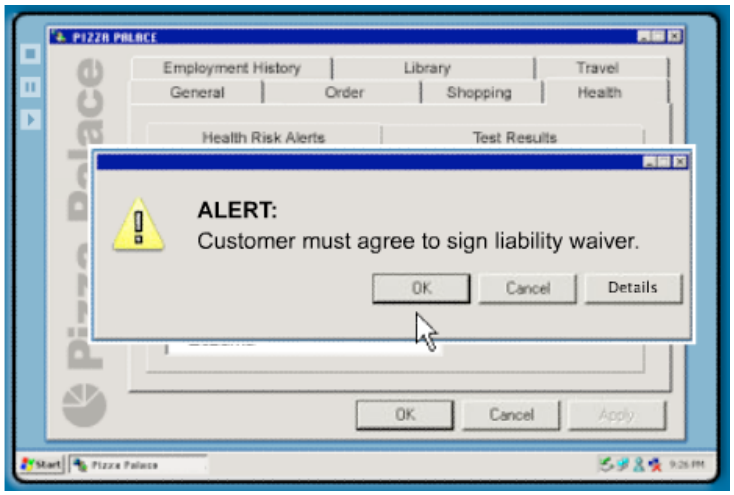
**System Audit:** Auditing mechanisms to verify privacy-compliant behavior of a system: This can include crowd-sourcing techniques such as a reputation system in which individuals can provide feedback about bad actors.

## External Compliance Testing and Certification

The popular concept of a "Personal Data Store" (or Personal Data Locker, or Personal Data Vault, or Personal Cloud, etc.) could be considered one of the prime examples of a piece of technology that implements several ideas in the above list. The purpose of Personal Data Stores is to securely hold personal data, as well as to use and share it in a privacy- and security-aware way. It can encrypt personal data. It can provide transparency by auditing access. It can anonymize personal data when necessary. Through practices such as "controlled push" and "informed pull", it can ensure that

personal data is collected and shared only with the express consent of the user.

A key strategy to achieve Privacy-By-Design is to simply limit the storage of personal data throughout one's entire architecture. Besides in "primary" storage components such as databases, copies of personal data may also appear in a number of other places. The following diagram (taken from a




presentation by Personal.com's CTO Tarik Kurspahic) shows a typical system design in which log files, backups, caches and other elements can contain traces of personal data and therefore have implications on the privacy characteristics of a system:

## Privacy By Design in PDEC

Within the PDEC Startup Circle, although the member companies tend to be rather different in their exact goals, every one considers privacy a key principle of their software design.

What do PDEC member say about Privacy-By-Design?

Qiy je digitale ik

All data in the Qiy infrastructure is encrypted. When individuals enter into a relation with an organization, they do so with pseudonymous identifiers, which prevents correlation. Also, personal data is divided from other data, therefore reducing the risk of tracing back leaked data to the person it belongs to. Qiy complies with the highest privacy standards in the Netherlands ("Privacy-Audit-Proof").

SYNERGETICS COMPETENCY DRIVEN KNOWLEDGE TAS3

In the TAS3 architecture, fully pairwise pseudonymization is used consistently both in the front channel (website) and the back channel (web service). By using pseudonymous tokens that are different for every session and every website or web service, one avoids correlation. Data is encrypted both at rest and in transit. Also, multiple "choke points" (PEPs – Policy Enforcement Points) in various places of the architecture enforce permissions and obligations.

## The Customer's Voice

The Customer's Voice perspective is that Privacy-By-Design is table stakes in the Personal Data Ecosystem we envisage; and that we are actually more focused on "Information Sharing by Design". This is what comes after the base protections are in place. In this mindset, the individual is acting as a point of integration for many other sources of data about them.

personal™

Personal, which in fall 2011 was named a Privacy-By-Design Organizational Ambassador, is undertaking a number of steps to ensure its users' privacy. Granular permissioning, transparent request and access records, as well as various encryption mechanisms contribute to this goal. Also, individuals ("Owners") are able to export their data and to permanently delete their account including all backups.

archify

The objective of Archify is to capture all sources of information that you have online. A range of measures is taken to let you control this process. For example, information is not stored if sensitive websites are browsed via HTTPS, if websites are on a blacklist, or if a private/incognito mode is enabled.

Privowny beta

With Privowny, personal data can be encrypted with a private key, which is protected by a security code. The private key is split into multiple parts, which are distributed among different servers and different legal entities. When the

private key is needed, it is reconstituted only locally, not on a server.

TANGLED
WEB COMMUNICATIONS

Tangled Web Communications provides mobile apps that work with a pure peer-to-peer model. In this model, all personal data is stored locally on one's device, and therefore all control lies with the user.

## Privacy-Enhancing Technologies (PETs)

While the principle of Privacy-By-Design refers to the general practice of designing software and architectures with privacy in mind, there is also a class of concrete technologies specifically created to enhance privacy. In the field of identity management, where traditionally an individual has to give up some of their privacy and provide credentials or attributes in order to prove their identity, an interesting set of cryptographic methods known as "minimal disclosure technologies" has emerged.

The most prominent examples of PETs are *Idemix* by IBM and *U-Prove* by Microsoft. They make it possible to provide proofs or attributes that may be required for certain transactions, while only disclosing a minimal amount of specific or identifying information, even to the point of complete anonymity. For example, when visiting a website targeted at minors, such technologies can make it possible to prove that you are under a certain age, and that you have parental consent, without however disclosing your actual age or your real identity.

Besides minimal disclosure, other features of these methods include the inability for a relying party to connect a credential to its issuer ("untraceability"), and the inability to correlate multiple uses of the same credential at the same relying party ("unlinkability").

The EU project "Attribute-based Credentials for Trust" (*ABC4Trust*) attempts to define a common, unified architecture for different minimal disclosure technologies, in order to allow comparing their respective features and combining them on common platforms. Its vision is to create a smartcard-based solution that provides built-in Idemix and U-Prove APIs.

## Beyond Technology

Remember that Privacy-By-Design is not solely about technology. It also involves legal and business practices, such as favoring opt-in agreements over opt-out, or anticipating and preparing for coming regulation on the use of personal data.

In addition, when it comes to the topics of security and privacy, it can often be heard that "users are the weakest link", which is a hypothesis that is the basis for many successful social hacking/engineering attacks. As a result, the role of individuals should also be considered an important element of Privacy-By-Design. This can mean simply educating users about privacy-sensitive functionality of a system. It can also mean providing them with effective and easy-to-use tools such as a personal data dashboard, a privacy manager, or a policy editor.

The design of default privacy settings should also be considered important. By default, personal data should automatically be protected, and only conscious actions by the user should change this.

To better communicate privacy characteristics to a user, initiatives such as the Standard Information Sharing Label can also be helpful, which aims to visually express how personal data is used by organizations.

## Conclusions

As individuals are becoming more conscious of their online privacy, the need for application of Privacy-By-Design principles by all service providers in the PDE will also increase. Embracing this fact will not only be a moral imperative, but also a concrete competitive advantage. Companies that provide individuals with tools to be in control of their personal data will be rewarded with trust and higher quality personal data.

Privacy-By-Design is really already a prerequisite for those of us who are working on building the PDE. Our next step will be to make good use of the vast potential for innovation that privacy-respecting architectures offer.

# NEWS

## Privy Torts

Jim Adler posted an interesting blog post on privacy culture clash across "The Pond." In his view The E.U. views privacy as a source "right of personality" versus the U.S. mosaic of privacy torts; the E.U. has comprehensive personal data law, The US, federal law is spotty, the E.U. has spotty enforcement at the nation-state level versus U.S. rigorous enforcement through private right of action, state enforcement through attorneys general, and federal regulation through the Federal Trade Commission.

http://jimadler.me/post/22382770205/privacy-a-transatlantic-culture-clash

## A Thousand Flowers Bloom in China

We spotted an interesting article on China's real names versus anonymous debate. Clearly, things are way more open in China than they used to be. But people remember the "thousand flowers bloom" of the Mao's years and know that identity comes at a serious price if the bill collector comes to collect. Real names on Weibo points to progress - People's Daily Online.

http://english.people.com.cn/90780/7681095.html

## The Key to Privacy at the ISP

This one also caught our attention. Nicholas Merrill fought and won against the data snoopers a few years ago. Now he sees a market for an ISP that protects user data to the limits of its energies, with privacy being its selling point, and end user controlled data encryption its method. Personal Data without encryption is just low hanging fruit.

This Internet provider pledges to put your privacy first. Always.

## Big Money for ID System

Optical Mouse Inventor and serial entrepreneur Steve Kirsch lands $7M in Series A startup money to create a secure key-based encryption mechanism and service for sharing personal data. Khosha and Northwoods led the investment.

http://techcrunch.com/2012/04/11/oneid-series-a/

## One More Time: WSJ Data Transparency Winners

In case you missed it, here is the list of winners in the Wall Street Journal's Data Transparency Weekend. Good companies to get to know from the New York Coding Party...

http://blogs.wsj.com/digits/2012/04/16/the-winners-of-wsjs-data-transparency-weekend/

## Is FaceBook 'Evil'?

This article breaks down the gauzy picture concerning how Facebook monetizes user data. Facebook's revenue is more than $130 per user/per year, and most of that income does not come from ads. According to the writer, the data, sold to aggregators who use then sell it to role players such as HR managers and others who investigate or track people.

http://open.salon.com/blog/steve_klingaman/2012/05/09/is_facebook_evil_yes

## Sold! An Auction Market for Personal Data?

We saw and read this HP paper on a personal data marketplace. Of course, there is a marketplace already... but it's a predatory one. Can a personal data "exchanged" be developed that balances out the rights of predators and prey?

http://cacm.acm.org/news/149089-a-stock-exchange-for-your-personal-data/fulltext

[*We tend to think it can. But wonder whether it can remain so if based upon a profit motive. All of the old stock exchanges were public corporations established for the common good and the exchanges were memberships with rules enforced by green-jacketed guys with teeth. All those exchanges are gone, replaced by computers, algorithms, and no-one minding the store. All you need is a nice $4 price spread on a market order by Bernie Madoff to see the problem...* -Ed]

## App Maker's Privacy Pledge on GitHub and Secure Mac Programming

Guidelines and efforts by app developers to address privacy are bearing awareness fruit. There are dozens of programmers on @github who have signed a secure programming pledge, and another effort has taken root in the Mac community.

https://github.com/iamleeg/privacy-pledge

http://blog.securemacprogramming.com/2012/03/more-about-the-privacy-pledge/

## Writer with Story about FTC Privacy Report Calls out Personal Data Ecosystem Contributions

"There are also three appendices that shouldn't be missed. The first is a year-by-year timeline of FTC "Privacy Milestones," starting in 1970. The second is a set of infographics depicting the "Personal Data Ecosystem." And the third is a spirited objection to much of the report, written by J. Thomas Rosch, one of the FTC's five current commissioners. "

http://smartdatacollective.com/brett-stupakevich/50556/ftc-report-puts-data-privacy-spotlight

## You Can't Get There from Here

Interesting article on Personal Data and Globalized Cloud Networks - Who Do You Sue?

http://www.pcadvisor.co.uk/news/security/3356704/if-offshore-cloud-compromises-your-data-well-sue-you-not-them-privacy-commissioner/

## Spam Texting Hits Mainstream Media

It all started with a text claiming the author could obtain a loan for $4500 in one day. But one bite of the noxious processed ham would beg for another tasty morsel...

http://www.forbes.com/sites/shelisrael/2012/05/09/and-so-it-begins-spam-text/

## Smile, You're on Candid Camera

The nature of miniaturized technology is that literally, you are always "on the air." As every president near a microphone has found out, they are always treated as on. So speaking of treatment, dentists in the UK are being warned that their patients are recording their consultations without prior notice, which turns out to be perfectly legal in the UK.

http://www.dentistry.co.uk/news/5089-Secret-patient-recordings-are-risk-to-dentists

## City of Sensors -- Portugal City Rises from the Earth with 100 Million Sensors

While we are not sure if the sensors include mood rings, this one takes the cake for the Singularity Creep Out of the Week.

http://www.alternet.org/story/155195/are_%26quot%3Bsentient_cities%26quot

## Personal Data Breach Complaints Changing

Security Recruitment Firm Barclay Simpson says that more complaints to the Personal Data Commission now reflect concerns about applications. "The report states that during 2011, the office opened 1,161 complaints for investigation, a record high when compared with the 783 grievances in 2010."

Access rights complaints (562) made up almost 50 per cent of the total, reflecting a growth in understanding of personal data security among the public. For the first time since the start of the report, the number of data breach notifications outstripped the number of issues opened for investigation, with 1,167 data security breach incidents reported to the office up from 410 in 2010.

http://www.barclaysimpson.com/personal-data-complaints-changing-news-2066/

## 13 Million Facebook Users Don't Change Open Access Privacy Settings

The sad part is, that this is by design. Simple, sensible, API design of privacy baked in. Zuckerberg has designed a machine that is designed to pry, take, and sell personal identities and their contents without compensation. Hence: PDE.

http://articles.nydailynews.com/2012-05-04/news/31576924_1_privacy-settings-privacy-controls-default-privacy

## EU Tries to Make People Prove Who they Are before On-Line Access

Although protecting children is easier if you ask them to read a book rather than surf the web, it's great that this same "protection system" can be expanded to deny access to those out of favor with only a change in policy.

[*The article is most noteworthy because it does not describe what the technology is or how it works.*-Ed]

http://www.newspakistan.pk/2012/05/05/EU-launches-plan-to-make-the-internet-safer-for-children/

## AlJazzera on Google's Existential Threat

Is Google in danger of becoming the next great has been, asks the Arabic network. It claims that Google's Social War on information control might be being lost. http://www.aljazeera.com/indepth/opinion/2012/05/201252154140601551.html

## Wikipedia's Next Big Thing: Wikidata

A Machine-Readable, User-Editable Database. An idea whose time is definitely come.

## Phil Windley: Personal Cloud

[The Cloud is the Computer. -Ed]

A great movement is underway where the computing power of a single device, connected as a slave to a master computer, might be giving way to a model where a complex but manageable array of services are connected and controlled by a user as a "virtual personal cloud." PDEC board member Phil Windley takes note of this in a series of blog posts. Worthy reading.

Post 1: http://www.windley.com/archives/2012/04/personal_clouds_as_general_purpose_computers.shtml

Post 2: http://www.windley.com/archives/2012/04/personal_clouds_need_a_cloud_operating_system.shtml

Post 3: http://www.windley.com/archives/2012/04/data_abstractions_for_richer_cloud_experiences.shtml

## SecureSafe Acquires US Competitor Entrustet to Expand International Reach

ZURICH, Switzerland, April 17, 2012 – DSwiss, founders of SecureSafe, the leading online data safe service, announced the acquisition of US-based digital estate planning service Entrustet. The acquisition will strengthen DSwiss' footprint within the US market and provide them with additional end users.

The service allows people to quickly, easily and securely prepare the last wishes for their digital assets and is a complement to SecureSafe's existing data inheritance features. By consolidating the two companies, SecureSafe (formerly known as DataInherit) becomes the premier service for offering high security data storage both now and for the future.

All existing Entrustet customers will be able to transfer their data to a SecureSafe account where they will not only benefit from the data inheritance features but also the invaluable file and password safes that can be accessed at anytime and anywhere via a PC or the services' free iPhone and iPad apps.

http://www.dswiss.com/en/dswiss-overview/news/securesafe-acquires-us-competitor-entrustet.html

## Maryland Bill to Prohibit Employers from Asking for Social Account Info

Maryland Steps Up to Trim the Desires of HR Managers who want your Facebook Password. But as articulated in an article above, key aspects of the content is already available to data aggregators via Facebook's other lines of business.

http://mlis.state.md.us/2012RS/billfile/SB0433.htm

## Arizona Internet Censorship Craziness

Arizona wants to prohibit speech on the internet from being anything impolite... and more!

The law is to apply to the Internet and other electronic communications. It would make it a crime to communicate via electronic means speech that is intended to "annoy," "offend," "harass" or "terrify," as well as certain sexual speech. However, because the bill is not limited to one-to-one communications, H.B. 2549 would apply to the Internet as a whole, thus criminalizing all manner of writing, cartoons, and other protected material the state finds offensive or annoying."

http://j.mp/H8lReN

## Tim Berner's Lee Steps Up on Data Rights: Demand your Data

The WWW inventor sees locked up value in personal data. He urges people to demand their Facebook and Google personal data. He sees on the horizon a new era of personal data services.

http://www.guardian.co.uk/technology/2012/apr/18/tim-berners-lee-google-facebook

## The Ethics of Attention

Very interesting piece on the ethics of communication in an age of wild abandon on the internet. Do we need a sheriff to ride into town, or just some fresh air and some decaf coffee?

http://www.ethanzuckerman.com/blog/2012/04/20/the-tweetbomb-and-the-ethics-of-attention/

### Tweet Ownership Hits the Alternative Mainstream Media

Judge says that Tweets do not belong to the Tweeter. Does that mean that Disney doesn't own Mickey Mouse?

http://www.salon.com/2012/04/26/who_owns_your_tweets/singleton/

### Do it Yourself Internet Takes Flight

Sacco and Vanzetti surely would love to have lived to see the rise of these digital freedom initiatives.

http://techland.time.com/2012/03/28/occupy-the-internet-protests-give-rise-to-diy-networks/

### FaceBook Stalker App Reviewed

Really great writing on the Facebook "stalker app" for the smartphone that served them up right on the screen. Truly creepy...

http://www.cultofmac.com/157641/this-creepy-app-isnt-just-stalking-women-without-their-knowledge-its-a-wake-up-call-about-facebook-privacy/

# Events

## 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

## FTC Mobile Privacy Workshop

**May 30**

Washington DC

http://www.ftc.gov/opa/2012/05/dotcomdiscl_ma.shtm

The workshop discussion will explore best practices for advertising and privacy disclosures. It will be used by Commission staff to update the Dot Com Disclosures guidance so that it better illustrates how businesses can provide clear and conspicuous disclosures in the current online and mobile world.

## 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.

## DataEDGE

**May 31-June 1,**

Shattuck Hotel, Berkeley.

http://dataedge.ischool.berkeley.edu/

"Educating the Next Generation of Data-Savvy Data Scientists." Every business, organization, and agency is going to need to understand and grapple with big data in order to thrive. The Information School at UC Berkeley is getting ready to train data scientists by launching its first annual conference, DataEDGE, which brings together experts in computer science as well as economics, medicine, sociology, and linguistics, to talk about the implications of big data in the workplace.

## Vibrant Data

**June 2**

**Portland, OR**

http://www.eventbrite.com/event/3399589263?ref=ebtnebregn

Imagine a world in which data becomes a personal asset that works on behalf of our personal interests and communities. At this event you'll pick a particular type of personal data and build an app to show how its value as a personal asset can be enhanced. The app can be mobile, desktop, web or something else.

## Singly Hackathon

**June 2**

http://www.hackweekends.com/events/singly_10000_hackathon.php

Join us for a weekend of food, beer and hacking. Bring a team or show up solo and form a team. You'll have all day Saturday and all day Sunday to build an app on the Singly platform, and the winning team will walk away with $10,000.

## Echelon 2012

**June 11-12, 2012**

National University of Singapore
Singapore, Singapore

Echelon 2012 is a two-day, double-track event on June 11-12 with over 1,100 delegates, a startup marketplace of up to 50 startups and various workshops. Echelon 2012 will be the biggest ever edition of Asia's best startup event. It will discover Southeast Asia's best startups on an all new scale. With lots of great projects underway in Singapore, they are earning their way to leadership in personal data.

## London Identity Unconference

**June 11, 2012**

London, UK

Following the internet Identity Workshop in California the community in the UK self organized an event to gather the community. Kaliya will be facilitating and attending.

## 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.

## New Digital Economics London

**June 12-13, 2012**

London, UK
www.newdigitaleconomics.com/EMEA_June2012/

The Communications, Media and Technology (TMT) ecosystem is becoming more complex as the business models of different players converge and collide. New Digital Economics Executive Brainstorms are premium strategy event focused on new growth opportunities and business models for TMT.

## Digital Enlightenment Forum

**June 18-19, 2012**

Luxembourg
http://www.digitalenlightenment.org/

The event aims to shed light on today's rapid technological changes and their impact on society and its governance. Kaliya is speaking about the Personal Data Ecosystem along with other notable industry leaders and some prominent regulators from Europe.

## Indie Web Camp

**June 30-July 1**

Portland, Oregon
http://indiewebcamp.com/Main_Page

Home of the "Indie Web" movement. Emphasis on building on the spot. Attendees must be "creators" who sign up with personal URL and OpenID, or apprentices to creators. Projects include IndieAuth

## (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

## Community Leadership Summit

July 14-15, 2012
Portland, OR
www.communityleadershipsummit.com/

Community managers from across open source, open standards, companies and communities gather and talk about their practice as community leaders. Kaliya will be attending.

## Cloud Identity Summit

**July 16-21, 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.

### WEF New Champions "Summer Davos"

**September 11-13, 2012**

China

The Re-Thinking Personal Data project will be doing programatic activity at this event. Kaliya will be attending.

### 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.

### W3C Federated Social Web Summit

October 22, 2012

Bay Area

This is official now the W3C will be collocating the 3rd Federated Social Web Summit near IIW. The day will have prepared presentations on the progress of these technologies ideas and then feed the results/energy into IIW.

### Internet Identity Workshop

**October 23-25, 2012**

www.internetidentityworkshop.com

Mountain View, California

This is the prime gathering for the User-centric and identity communities. It is the place where a huge amount of industry progress happens.

# Event Report

## The European Identity & Cloud Conference (EIC)

Organized by analytics firm KuppingerCole the EIC took place in Munich from April 17-20. This major event again brought together technologists, analysts and policy makers from all over the world. Like every year, EIC touched on a number of different identity-related areas, such as online Identity and Access Management (IAM), government-issued IDs, standards development, cloud security, and others.

Some of the concepts that received significant attention during the conference were::

Life Management Platforms: Such platforms are a superset of Personal Data Stores and will not just store personal data, but also provide individuals with useful services based on it, enabled through mechanisms such as "controlled push" and "informed pull".

API Economy: With the rise of cloud computing, the importance of API-based communication between service providers will also increase.

Several workshops about Identity and Security in cloud computing were held. It was mentioned that in the future, identity in the cloud will likely be based either on a monolithic identity provider holding all personal data, or on the idea of an Identity-Management-As-A-Service (IdMAAS) system that can assemble claims from different sources.

Privacy-By-Design and Minimal Disclosure Technologies were also discussed, for example their possible application on smartcards or by governmental ID programmes in Australia, New Zealand, or by the European STORK interoperability project.

Workshops on Key Internet Identity Protocols gave overviews of the current status of OpenID Connect, OAuth 2.0 and the idea of an Account Chooser, i.e. a standardized UI for web browsers.

A session about Doc Searls' The Intention Economy explored how this new paradigm will unfold and what underlying infrastructure and business models it will require. PDEC Startup Circle member Connect.me announced the launch of the Respect Network and its Founding Vendor's Program, which is aimed at taking the first step toward realizing the vision of the Intention Economy.

Participants of the conference were given two research reports by KuppingerCole. One "Scenario" report about "The Future of IT Organizations" examined the role that cloud computing will play in organizations' IT infrastructure in the future. And one "Advisory Note" explained the concept of "Life Management Platforms" in detail. The final highlight of the conference was the European Identity Awards ceremony. One of the awards was given to the OpenID Connect standard. On the conference's agenda page, some of the presentations are available for download, and video material is being added.

# Standards

## Unhosted: Security Consideration

**April 3 2012**

The Unhosted project - which is working on an architecture to separate data from apps on the web - has begun to formulate security considerations and possible threat models. This could also serve as an inspiration for other initiatives in the PDE.

## W3C: CORS published as Last Call Working Draft

**April 3 2012**

The W3C WebApps WG and WebAppSec WG have announced the publication of Cross-Origin Resource Sharing (CORS) as a Last Call Working Draft. CORS enables client-side web applications to make calls to APIs from sources other than the source of the web application itself, which is normally prevented by security restrictions of user agents. In the PDE, this might affect use cases in which applications access personal data from multiple sources. The deadline for comments to the draft is May 1st.

## OASIS Interoperability Guidelines

**April 3 2012**

A new whitepaper, "Interoperability Guidelines", has been published by the OASIS Technical Advisory Board (TAB). The whitepaper covers best practices for writing specifications in ways that minimize the risk of interoperability failures between implementations. It points out the most common traps that specification writers can avoid to minimize risk of misunderstanding. The target audience for the white paper is primarily specification writers and Technical Committee (TC) members.

## OASIS Nominations for Board of Directors and Technical Advisory Board

**April 3 2012**

Nominations are now being accepted for the OASIS 2012 Board of Directors and Technical Advisory Board elections. Members will elect six candidates for seats on the OASIS Board of Directors and two candidates for seats on the Technical Advisory Board. Each will serve a two-year term beginning July 2012.

## OASIS Identity in the Cloud: Public Review of Use Cases Version 1.0

**April 5 2012**

The OASIS Identity in the Cloud TC has produced an updated Committee Note Draft (CND) of its Cloud Use Cases Version 1.0 document and submitted it for public review. The document as well as supporting files are available as a ZIP package. It is intended to provide a set of representative use cases that examine the requirements on identity management functions as they are applied to cloud based interactions.

## IETF: The Canonical Link Relation

**April 6 2012**

For the PDE, it will be important to have a mechanism for referring to individuals and organizations, as well as to relations between them in a stable and reliable way. Building on RFC 5988 (Web Linking), a new RFC 6596 is now available that describes a canonical link relation, i.e. one that is considered the preferred among multiple relations between resources. This could be a useful building block for personal data relations in the PDE.

## OpenID Connect: Web Intents for Discovery

**April 9 2012**

Web Intents is an HTML5 feature that enables client-side service discovery. On the OpenID Connect list, a suggestion has been made that Web Intents could be used to discover a user's OpenID Connect provider. Developer Nov Matake has deployed slides and a demo implementation that explain how exactly a provider and relying party can use Web Intents for the discovery aspect of OpenID.

## W3C Web Cryptography Working Group

**April 9 2012**

The W3C launched a new Web Cryptography Working Group as part of its Security Activity. The mission of the new working group is to define an API that lets developers implement secure application protocols on the level of Web applications, by exposing trusted cryptographic primitives from the browser. Its charter explicitly mentions the necessity to perform high-value transactions such as those involved in identity-related claims about personal data. Since several PDEC Startup Circle members are already encrypting personal data today, the output of the new working group is likely to become highly relevant.

## OpenID Connect Update Release

**April 10 2012**

OpenID Connect Work Group has released an update to the OpenID Connect specifications that continues incorporating significant developer feedback received. The specs have also been updated to track updates to the OAuth and JOSE specs, which they use. The new versions are available from http://openid.net/connect/.

## W3C Big Data Community Group Created

**April 10 2012**

A new W3C Community Group about "Big Data" has been created, stating that it will "explore emerging BIG DATA pipelines and discuss the potential for developing standard architectures, Application Programming Interfaces (APIs), and languages that will improve interoperability, enable security, and lower the overall cost of BIG DATA solutions".

## Webfinger vs Simple Web Discovery

**April 12 2012**

On the OAuth mailing list, an intense discussion has began on the respective advantages of the Webfinger discovery protocol and of one of its alternatives, Simple Web Discovery (SWD). As we pointed out in Issue #1 of the Personal Data Journal, Webfinger has for while been regarded as the de-facto standard for discovery on the web. OpenID Connect Discovery however is currently based on SWD. The arguments on the list are based on static content vs. dynamic lookup, XML vs. JSON, privacy characteristics, and ease of implementation and deployment. While the outcome of the discussion is currently uncertain, it is likely to have a strong impact on many communities including the PDE.

## IETF: OAuth Use Cases

**April 12 2012**

A new Internet draft has been submitted to IETF to list 13 OAuth use cases, which are based on the Internet drafts of the OAuth working group and discussions on the group's mailing list.

## OpenID Connect Webinar & Java/Spring library

**April 12 2012**

Justin Richer, Lead Technologist of MITRE Corporation, has held a webinar at the MIT Media Lab about OpenID Connect. The slides and audio recording are available online, as is a new Java/Spring implementation for OpenID Connect.

## Python UMA (PUMA) library released

**April 16 2012**

A first version of a Python implementation of User-Managed-Access (UMA) has been released. As we explained in Issue #2 of the Personal Data Journal, UMA builds on OAuth 2.0 to provide a way for individuals to manage all access to their personal data and services in a centralized manner. The PUMA projects also contains examples and slides to explain different sharing scenarios.

## OpenID Connect wins EIC Award

**April 18 2012**

At this year's European Identity Conference (EIC), OpenID Connect won the European Identity Award in the category "Best Innovation / New Standard in Information Security". It was recognized as an important authentication standard that meets today's requirements on the Internet and cloud environments.

## Kantara: Working Draft 0.1 of the Standard Information Sharing Label

**April 22 2012**

Joe Andrieu (SwitchBook), Iain Henderson (The Customer's Voice) and Judi Clark (WomensWork) have produced a working draft document of the Standard Information Sharing Label. This label visually expresses how personal data is used online by organizations, and it constitutes a simple alternative to complicated Terms of Use and Privacy Policies.

## PubSubHubbub: Comments on Spec V0.4

**April 23 2012**

On the PubSubHubbub (PuSH) W3C Community Group, several individuals have sent feedback about the latest 0.4 version, e.g. on this blog post, or in this message to the mailing list. One of the points is that PubSubHubbub should support arbitrary content instead of being focused on RSS/Atom feeds, which could be useful for transporting personal data in the PDE. Another open question is to what extent identity and authorization mechanisms should be built into PuSH.

## REST Profile of XACML v3.0 Version 1.0

**April 24 2012**

The OASIS eXtensible Access Control Markup Language (XACML) TC has published a draft document defining Restful services for XACML. One of the uses cases described in this document is to provide Authorization-as-a-Service functionality.

# Startup News

The Startup Community has expanded with a new group of almost 10 companies. We are introducing them in this and the next issue.

## New Members!

Planetwork is building a Citizen Cloud to serve the needs of people from overlapping communities of purpose, place and practice. Non-profit organizations that need a shared social network will offer it to their members. Private companies that provide tools and services will benefit from early adopters. Planetwork will use the OIX Trust Framework to create a legally binding shared privacy policy. Once a large network of people control their data, the network will offer a VRM relationship to companies that wish to access the network. Planetwork is a San Francisco based non-profit that published the ASN White Paper in 2003. planetwork.net

Privowny empowers consumers to create their digital memory, manage their personal information and market this information from a single platform that only they control." privowny.com

"Lifedash is a social privacy platform created for users to control and share data privately. Lifedash personas allow users to create multiple profiles that align with the various roles they play in day-to-day life, while managing and sharing data across useful applications." lifedash.com

At Allfiled we believe that individuals will become the best point of integration and origination for data that relates to them; we provide tools and services that will help this change come about. This will have significant impact on the relationships between individuals and their suppliers, with both parties having much to gain from this shift. We have been providing personal data services since 2007, and plan to re-launch an upgraded service in 2012. allfiled.com

## News...

**Respect Network Corporation** reports that Connect.Me, its socially-verified reputation network, will shortly move from private to public beta with a new much more scalable back-end and a developer API.

**Respect Network Founder's Program was Launched**, the first step in inviting companies to join the Respect Network and begin forming true VRM connections with Connect.Me users under the umbrella of the Respect Trust Framework. Respect Network architects include **Doc Searls, Phil Windley, Craig Burton, Scott David, Iain Henderson, Alan Mitchell, and Jim Fournier. Consulting Partners include Ctrl-Shift, The Searls Group, and Burtonian. Non-profit partners include Planetwork and Bitworld.** See the new website at respectnetwork.com for more details.

## Singly Raises $7Million from SV Venture Investors

The Wall Street Journal is reporting that Singly, a PDEC member, raised $7M in a Series A funding led by Foundry. New Singly angel investors, along with Foundry Group, include Robert Stephens, the former CTO of Best Buy; Federated Media's John Battelle; Esther Dyson; and Roger McNamee. Previous seed investors included Venrock, True Ventures, PivotNorth Capital (Tim Connors) and Freestyle Capital.

Singly is an API that offers to share personal data in a manner that is respectful to the user. They have few users yet, but have a serious development effort underway and amazing prospects. Note the pedigree of previous and new investors

and you'll see the smart money clamoring to get an early piece of this wonderful PDEC company.

personal™

## Personal iPhone App! Finally :)

The latest: a their new IOS app for Ipad and Iphone. So it's personal....and now it's portable.

This is big news. The Personal App allows personal customers to control and manage their personal information on the device and extend privileges to others they trust. Think of it as the enterprise identity console for everyone. Of course it directs the services of the personal service at personal.com. As a user of many apps that direct internet services, I disdain having to go to the browser to get things done. Great work here. And its available free on the Apple App Store.

http://www.businesswire.com/news/home/20120507005284/en/Personal-Launches-iPhone-App-People-Safely-Store

http://blog.personal.com/2012/05/personal-for-iphone-how-i¹m-using-our-newest-mobile-app

http://gigaom.com/2012/05/07/personal-lets-people-get-the-most-of-their-small-data/

http://techcrunch.com/2012/05/07/personal-takes-its-secure-vault-for-all-of-your-private-digital-data-mobile-with-ios-app/

http://www.fastcompany.com/1836521/personalcom-creates-an-online-vault-to-manage-all-your-data

## Trust Fabric is now in Beta.

TrustFabric

The VRM service gives users a seat at the table with vendor relationships. Here are a several of stories covering this.

**Related stories:**

http://www.gadget.co.za/pebble.asp?relid=4527

http://mybroadband.co.za/news/general/47560-spam-opt-out-lists-trustfabric-versus-dmasa.html

http://www.itweb.co.za/index.php?option=com_content&view=article&id=53395

http://www.bizcommunity.com/Article/196/14/73656.html

http://www.bandwidthblog.com/2012/04/13/trust-fabric-opt-out-service-mxit/

http://www.swimgeek.com/blog/2012/04/16/opt-out-article-in-die-son/

*TrustFabric is a VRM community company but is not yet a startup circle member.*

# Resources

## Global Information Technology Report 2012

World Economic Forum

wef.ch/gitr2012

New WEF Report Underscores the promise, patience, and some of the peril of the I-Renaissance. This is a big, broad, and important collection of some of the most important trends in internet society. It covers availability, network neutrality, Big Data, "The Wisdom of the Cloud", the Value of Digital Traces for Commercial Strategy and Public Policy, The Promise and Peril of Hyperconnectivity, Maximizing the Impact of Digitalization, Technology Use in Education, Case studies for ICT for Competitiveness and Well-Being, I-nation building (the case of Mauritius), some great data on countries (see the screen shot), written by scholars at the National Academy of Sciences, CRESCI, and McKinsey.


Here is a screen shot of the data tables by country. [Nothing like a little light on a subject to get people moving. -Ed]

http://www.edelmandigital.com/2012/04/05/privacy-security-the-new-drivers-of-brand-reputation-and-action/

## Digital Differences

When the Pew Internet Project first began writing about the role of the internet in American life in 2000, there were stark differences between those who were using the internet and those who were not. Today, differences in internet access still exist among different demographic groups, especially when it comes to access to high-speed broadband at home. The ways in which people connect to the internet are also much more varied today than they were in 2000. As a result, internet access is no longer synonymous with going online with a desktop computer.

http://pewinternet.org/Reports/2012/Digital-differences.aspx

## The Future of Money in a Digital Age

Within the next decade, smart-device swiping will have gained mainstream acceptance as a method of payment and could largely replace cash and credit cards for most online and in-store purchases by smartphone and tablet owners, according to a new survey of technology experts and stakeholders. Many of the people surveyed by Elon University's Imagining the Internet Center and the Pew Research Center's Internet & American Life Project said that the security, convenience and other benefits of "mobile wallet" systems will lead to widespread adoption of these technologies for everyday purchases by 2020.

Others—including some who are generally positive about the future of mobile payments—expect this process to unfold relatively slowly due to a combination of privacy fears, a desire for anonymous payments, demographic inertia, a lack of infrastructure to support widespread adoption, and resistance from those with a financial stake in the existing payment structure.

Read or download the full report: http://pewinternet.org/Reports/2012/Future-of-Money.aspx

## Personal Cloud White Paper by Phil Windley and Drummond Reed

http://www.windley.com/cloudos/cloudos.pdf

One of the most important themes to come out of IIW was the idea of the Personal Cloud. Phil covers the Cloud OS, some of the nomenclature, models, and a great discussion of the emergence of a broad structure of personal clouds. We highly recommend this report. Interesting reading.

## Verizon Data Breach Investigations Report

"Information Security Service and the Police Central eCrime Unit of the London Metropolitan Police. This collaboration is important because this is a global issue: About 70 percent of the data breaches originated in Eastern Europe and 75 percent originated outside of the United States. The Data Breach Investigation Report (DBIR) series now spans seven years and more than 2,500 breaches involving more than one billion compromised records, making it the most comprehensive study of its kind. Through our Data Breach Investigations Report series, Verizon continues to provide the industry with a first-hand look at cybercrime around the globe. Verizon offers this report free because we believe education can significantly help organizations protect themselves against cyber attacks. For example, this year's report found that 97 percent of the data breaches could have been avoided without the need for organizations to resort to difficult or expensive countermeasures."

[Nice article to gather referencable data on breaches. Could be useful PPT ammo -Ed]

www.verizon.com/enterprise/2012dbir/us

## Looking Back at P3P: Lessons for the Future

A number of people who work on data protection have begun examining the idea of machine-readable statements that can express the privacy practices of a Web site or a third-party intermediary, such as a network advertiser or an analytics company. The theory is that such statements would provide a clear, standardized means of rendering potentially complex privacy policies into a format that could be automatically parsed and instantly acted upon.

The Platform for Privacy Preferences (P3P) is a standard of the World Wide Web Consortium (W3C), the main standard setting body for the Web. P3P has never been fully implemented as its creators had hoped. While it is in use today and functions in some ways as we thought it might, P3P is unlikely to be broadly adopted or to accomplish all that those pushing for machine-readable policies would like.

https://www.cdt.org/paper/looking-back-p3p-lessons-future

An interesting article on why Facebook's IPO matters to women. The article covers corporate board representation and has a lot of data on the status of women in corporate america.

http://www.women2.org/why-facebooks-ipo-matters-to-women-seven-white-men/?utm_source=email

Gartner

As we mentioned in the News section, *personal clouds* are becoming a hot discussion and development area. Gartner agrees and has created an in-depth report on the topic. The report says:

> The personal cloud is poised to eclipse the PC as the hub of consumers' digital lives by 2014 as rapid growth in the use of apps and services introduces a new paradigm for how people store, synchronize, share and stream content, according to Gartner, Inc. "The personal cloud isn't a single offering, but a reflection of consumers' expectation that their content will flow seamlessly as the result of a combination of services that overlap the consumer, business and government domains. It encompasses content storage, synchronization, sharing and streaming, as well as context-based access," said Michael Gartenberg, research director at Gartner.

Gartner Personal Cloud Report. ( $1295 for full report)

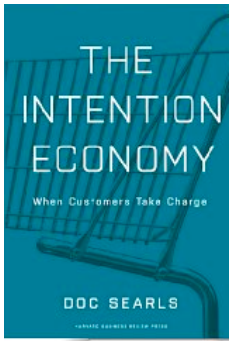
http://www.gartner.com/it/page.jsp?id=2008517

## Video of the Month: Google Street View Wifi Program by WSJ


Dinosaur Media feels the heat coming off the Google hush program that got outed. What is interesting here is what is not said... like how the information was being used...

http://www.youtube.com/watch?v=4bI1N9VZHNA

# Book Review




## The Intention Economy

### When Customers Take Charge

### by Doc Searls

### Review by Kelly Mackin

314 pages. $16.20

search for it

*Disclosure: Doc Searls, the book's author, is a PDEC advisor.*

Before the middle of the last century, economics was called political economy. With the rise of computing and advanced statistical techniques after World War II, political economy gave way to econometrics and the rise of quantitative analysis. Political economy was always a broader, and in my opinion better, subject than its descendants for it allowed writers to connect economic thinking to the broader societies and issues that it directly affects.

Working on a three-year fellowship at the Berkman Center for Internet and Society, Doc Searls, an award-winning writer and journalist, has been spearheading a deep and important project on the role of intention in the structure of human action. His project centers on the development of an intellectual and technology consensus to develop a political economy of the web. The internet was created by by engineers who cared more about creating things and worried less about making money.

Searls points out that the "open" internet is now overshadowed by the web as a sort of a Blade Runner "shopping mall." Relationships in this commercial web are governed by an essentially feudalistic rubric where sellers - in their crush to maximize revenue streams - essentially control all the material terms of a relationship. This feudalistic model developed in the absence of a technical infrastructure that would support other models.

As in the case of proprietary email systems, the need exists to develop interaction methods that support a 1:1 correspondence between buyers and sellers. In the current model, by promoting *adhesion*, where sellers enforce a take-it-or-leave-it model that attempts to control the customer. Adhesion strongly encourages or even enforces customer actions that benefit the seller more than the buyer.

In Searls' view, the commercial web arose as a consequence of the Taylorist viewpoint that the holistic person or entity that is seeking something matters only for behaviors that support the goals of the seller. This model creates all manner of problems and he devotes over 150 pages of the book to trace the history of networking and the evolution of commerce in the last century to show how we arrived at this point.

Searl's does a superb job laying out the development of the quiet technologies that underlie the web and convincingly shows that the nature of these open systems enables players on the web endpoints to share without the permission of players in the center who supply connectivity. The bright group of developers and thinkers who animate this quiet internet, who create the structures that the success of the internet relies upon are now bringing these principles into operation at the service level.

Examples abound, but one of the best is Personal's approach to fourth party services. Personal declares in their legal agreement that the customer is the owner of their data. Alan Mitchell of CNTL-Shift, the founder of MyDex, led the charge in Britain to embody similar principles and has gotten the support of many companies and government officials in England. [Personal is a PDEC member -Ed]

Searls' model is an attempt to reform the commercial web with technologies and services that enable the internet's open systems principles to rise to the level where they can change the dynamic between customers and sellers, between publishers and readers, and any other scission where the balance of control rests squarely in the laptop of the more powerful interest.

Personal Vendor Relationship Management is tightly defined in the tract with a set of principles that follow from a belief that the 'free' customers are more valuable than captive ones. For those new to pVRM, the principles (from the project's website) are:

- Customers must enter relationships with vendors as independent actors.
- Customers must be the points of integration for their own data.

- Customers must have control of data they generate and gather. This means they must be able to share data selectively and voluntarily.
- Customers must be able to assert their own terms of engagement.
- Customers must be free to express their demands and intentions outside of any one company's control.

In the book, these principles are described at the end of the chapters. On the future relationships of customers to sellers, he says:

> *"Relationships between customers and vendors will be voluntary and genuine, with loyalty anchored in mutual respect and concern, rather than coercion. So, rather than "targeting," "capturing," "acquiring," "managing," "locking in," and "owning" customers, as if they were slaves or cattle, vendors will earn the respect of customers who are now free to bring far more to the market's table than the old vendor-based systems ever contemplated, much less allowed."*

There is an intense social meme recently that fairness has to be the basis of any sustainable political system. The question and the rub is always how fairness is to be achieved. Is fairness to be achieved by the actions of government to regulate, control, (and thereby distort) economic activity, or is it better achieved by enabling participants to thoughtfully manage their participation by giving them tools and services that allow them to have an equal seat at the market table? This of course leads to a discussion of the idea of the commons.

The venerated economist Adam Smith, in his book of political economy, "The Wealth of Nations" was promoted as an intellectual tour de force at the time of its publication and thereafter. But, as many economists have pointed out, Smith's distorted and incorrect analysis of the "problem of the commons" was used to justify and cement control mechanisms of monied interests that were opposed to self organization and the idea of the commons. Searls correctly points out that in the UK, the commons has altogether disappeared; replaced by private control. To a great degree, says Searls, the web in the commercial sphere has fallen victim to feudalistic structures in a similar way, although at the network and protocol layers, this openness still mostly operates.

> *"For free markets to mean more than "your choice of captor," we need new systems that operate on the principle that free customers are more valuable—to both sellers and themselves—than captive ones. Improving slavery does not make people free. We need full emancipation. That's the only way we'll get free markets worthy of the name."*

This is a groundbreaking work, full of mentions of fellow travelers and chock full of earnest work designed to help people participate fully as sovereign individuals within the internet sphere. It would not surprise me if one day this will be seen as a book as venerated in internet circles as Adam Smith's was in the temples of the elite. Perhaps another title could have been, "The Wealth of Internets."

Recommended.

# Special Report

## FTC Privacy Report Review

### by Kaliya Hamlin

**"Protecting Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers."**

The report, in addition to its other purposes, contextualizes the history of the FTC involvement in issues of consumer privacy since the passage of the Fair Credit Reporting Act of 1970. An *Appendix A* covers major Laws & Rules, Cases, Reports, Workshops and Educational efforts since then.

The report outlines key developments including a whole list of enforcement actions against Google, Facebook and online ad networks that do not respect opt-outs and mobile apps that violate COPPA. It has hosted two privacy-related workshops and FTC executives have on nearly a dozen occasions given testimony before Congress.

The report calls for delineation and implementation of best practices to "make privacy the default setting." It calls for consumers to be given control over the collection and use of their personal data held by enterprises along with simplified choices and increased transparency.

> *"To reduce the burden on those consumers who seek greater control over their data, the proposed framework called on companies that collect and use consumer data to provide easy-to-use choice mechanisms that allow consumers to control whether their data is collected and how it is used."*

The authors of the report clarified the practices that do not require choice:

(1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing.

The five major foci of the report are: Do Not Track (DNT), Mobile, Data Brokers, Large Platform Providers and Self Regulatory Codes.

### DNT

PDEC replied to preliminary version of the FTC report released in December 2010 challenging the premise of Do Not Track and suggesting a more forward-looking pro-business pro-consumer path would be to support netizens being empowered to collect their own data. Our response was not referenced in the report.

The direction proposed in the report endorses Privacy by Design (see feature in this issue) meaning that privacy is built in at every stage of product development. The FTC are also keen on the W3C's development of Do Not Track mechanisms and the CAA's opt-outs for behavioral advertising along with agreeing not to share consumer data to third parties for secondary purposes.

The report states emphatically that businesses should provide a Do Not Track Mechanism To Give Consumers Control Over the Collection of Their Web Surfing Data.

### Mobile

The Report draws particular attention to the issues around Mobile technologies and has a whole "box pull" on the subject. On page 33, the section concludes with the following statement, calling for the entities involved in the mobile ecosystem to work together:

> *"With respect to the particular concerns of location data in the mobile context, the Commission calls on entities involved in the mobile ecosystem to work together to establish standards that address data collection, transfer, use, and disposal, particularly for location data. To the extent that location data in particular is collected and shared with third parties, entities should work to provide consumers with more prominent notice and choices about such practices. Although some in the mobile ecosystem provide notice about the collection of geolocation data, not all companies have adequately disclosed the frequency or extent of the collection, transfer, and use of such data."*

Events are moving rapidly in the field and the FTC is hosting a workshop on May 30th in DC to cover mobile privacy issues specifically and encourage the conversation about self regulation. It will be webcast

### Data Brokers (DB)

DB are companies that collect information about consumers from a wide variety of sources for the purposes of converging and reselling the information. Their customers use the information for various purposes including identity verification, differentiating records, marketing products and preventing financial fraud. Consumers do not interact

directly with these organizations and the report said that this needs to change with the provision of "special access mechanisms for data brokers" because "consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data." This approach suggest something similar to consumer credit agencies that offer consumers services that enable them to manage their credit.

## Large Platform Providers (LPP)

The inclusion of an LPP category and the issues that surround it was a key enhancement to the structure of the project.

> *"ISPs are thus in a position to develop highly-detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible... The Commission also recognizes that the use of cookies and social widgets to track consumers across unrelated websites may create similar privacy issues....*
>
> *These are complex and rapidly evolving areas and more work should be done to learn about the practices of all large platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data."*

The FTC report highlights many of the issues including "Take-it-or-Leave-it Choice for Important Products or Services Raises Concerns When Consumers Have Few Alternatives" The issues for this class of service provider remain unresolved and they are planning on hosting a workshop focused on this area in the 2nd half of 2012.

## Self Regulatory Codes

The FTC is encouraging industry to set best practices for these various ares of concern.

Other things of interest in the report include a pull out box on page 41-2 focused on the emerging new field of facial recognition and its application in retail (and other) situations.

> *"This surge in the deployment of facial recognition technology will likely boost the desire of companies to use data enhancement by offering yet another means to compile and link information about an individual gathered through disparate transactions and contexts....*
>
> *"A recent paper from researchers at Carnegie Mellon University illustrated how they were able to combine readily available facial recognition software with data mining algorithms and statistical reidentification techniques to determine in many cases an individual's name, location, interests, and even the first five digits of the individual's Social Security number, starting with only the individual's picture...*
>
> *The ability of facial recognition technology to identify consumers based solely on a photograph, create linkages between the offline and online world, and compile highly-detailed dossiers of information, makes it especially important for companies using this technology to implement privacy by design concepts and robust choice and transparency policies. "*

To underscore the problem raised by the FTC, the CIO of Seattle, Bill Schrier, said at the Privacy, Identity, and Innovation Conference in Seattle that "facial recognition is the greatest danger to privacy that we've seen so far."

There was a long conversation in the document about whether the enhancement of data that is collecting information about a person doing some activity and then buying data form another source to "enhance" the data about the person and thus enable better targeting was an acceptable industry practice.

They also clarified what in their view is the difference was between first and third party tracking on the web stating that "Affiliates Are Third Parties Unless The Affiliate Relationship Is Clear to Consumers."

The framework also calls for consumer choice where a company shares with a third party the data it collects from a consumer. Thus, consumers will have the ability to control the flow of their data to third parties who might sell the data to others for enhancement.

What this report does not do is call for the regulation of data usage. It still is focused on practices of collection and control for consumers in that process. Once collected the consumer looses control and is not protected, and has little recourse.

# Opinion

## Framing The Personal Data Ecosystem

By Allan Friedman

*[This is the first of a series of articles in coming issues that address the evolution of the ecosystem. -Ed.]*

How we talk about an issue can shape our positions, agendas, and how we seek and identify solutions. This is known as "framing," and its been studied in everything from behavioral economics to opinion polling. Psychologists Daniel Kahneman and Amos Tversky famously pointed out that the same questions will induce different questions if they are framed as a loss or a gain. As a simple example, the "death tax" is substantially less popular than the "estate tax." And it is the concepts that we apply to topics that enable and inhibit thinking. It is as if the frame itself is a key element in boosting the probability of one result, or reducing another. Essentially, with framing we are, unconsciously or not, engaging in a social engineering of the result.

A more subtle effect of framing is to guide our approach to thinking about and thus addressing key issues. For example, when we talk about 'identity theft,' we rely on mental models of theft, which drives products that protect data and prevent data loss, business models around shredding papers and safeguarding secrets. But if we look at the same issue as 'fraud,' there are a host of other tools we might bring to bear, looking at the challenges of authentication and the ability to detect misuse. It is not that these views are mutually exclusive, but the way these issues are framed can drive different approaches. The process of frame analysis can be beneficial in that we have a broader set of perspectives and solutions. The risk to the goal is that by failing to appreciate the implications of particular frames, proponents of different perspectives will continue to talk past each other and communities will fail to cohere.

I'm fascinated by the growth of the Personal Data Ecosystem because so many different issues in technology policy seem to drive towards towards rethinking personal data. But these different paths each come with their own frame. I've seen brilliant people begin discussions by framing PDE as a solution to the problem of privacy, a question of fairness, a critical component of an evolving digital lifestyle, a means of matching customers and solutions, or a far more efficient way to mine data. These discussions are often productive, but can be followed by a similar discussion with a different frame that feels completely detached from the metaquestion of what should we achieve.

Even inside a narrow issue, such as health data, starting from different perspectives can make a difference. While researchers have been intrigued by the power of using electronic health data for research, the first paper suggesting an independent health vault in 1997 was proposed as a data security solution to limit access. An emphasis on making sharing easier for personalized medicine, or access easier for evidence-based medicine does not mean that engineers and entrepreneurs aren't sensitive to the privacy issues, but that they are focusing on enabling sharing. But even with the mutual focus on sharing, the agenda of a VRM proponent will have different priorities than a data miner.

In a future article, I'll explore further areas of conflict between these different discussions, and try to identify clear areas where different understanding of the issues in PDE can lead to zero-sum games and potential conflict. But I think its important to recognize the up side of having so many people approach PDE from different perspectives. This diversity inevitably leads to a proliferation of approaches, solutions, and the basic building blocks that will evolve as the ecosystem grows and matures. But for this cross-fertilization to be successful, we all have to be aware of how others frames may interact with our own perspectives. And successful innovators in this space will be able to frame their solutions in terms so that others can understand their value.

*Allan Friedman is a fellow in Governance Studies and research director of the Center for Technology Innovation at Brookings. His current research focuses on information technology policy, with particular emphasis on cybersecurity policy and the dynamics of information privacy.*

# Publisher's Note

## Dignity and Data

### by Kaliya "Identity Woman" Hamlin

The buzz about the buzz-phrase "BIG DATA" continues to escalate. Two years ago I co-convened the Big Data Workshop, an unconference focused on the various database technologies being developed to handle large data sets. One of the things I found most striking was that in two days and almost three dozen sessions being convened only one touched on the fact that much of the data was generated by people as they lived their lives and therefore there were social, ethical and rights implications that had to be considered. The guys who were handling these data sets were almost completely oblivious to the source of the data.

I have heard it said in this era of Web 2.0 and now Big Data that the social web and tracking technologies that are pervasive, generating lots of data and are good for business are also harmless to users (who are people). When those building these systems do become aware of the source, the issues that come under the umbrella label of privacy are dismissed. Just this week at the Future of Money and Technology conference I heard several off hand comments made by young male programmers at this week that privacy was "dead." The community working on user-centric identity tools and technologies and now the related but distinct community working on personal data services has always challenged this notion that these practices are "harmless."

I do think that privacy as secrecy and the current frame of how privacy is considered in much of the legal and policy discourse is outdated because it doesn't reflect what is realistic in digital systems today. However to dismiss the core reasons why people are concerned about issues under the umbrella of the term "privacy" will undermine this emerging industry.

One of the key issues that people use the word privacy to express concern over is human dignity - that is respect for the individual relative to particular context and impersonal bureaucratic and business systems.

In human social groups and systems we share with each other information based on how well we know people. Each of us keeps some of this information we know about others in confidence so as to safeguard dignity. An example might be that we share with a few close friends the details of a major illness we have with the understanding that they not disclose the specifics to a wider group but may disclose that we are indeed ill.

These social norms for sharing are not guided by the law but they do help us create safe space for sharing with each other. Some sharing and transactions are protected by law - what we disclose to our doctors in the doctor-patient relationship and what movies we rent from a video store or books we lend form a library. These are protected so we have the freedom to go and explore new ideas and interests without them being disclosed in appropriately in ways that undermine our dignity.

If we as an industry start to hold up human dignity as a key value we share then we can have discussions about normative systems and uses for data that maintain and uphold dignity and ones that don't. The conversation about data can move to one about appropriate and inappropriate usage rather then be bogged down in a quagmire about "privacy" and protecting it by preventing any data collection.

Data are a byproduct of our modern digital life and regulating collection but not usage is off the mark. Last week I attended my first World Economic Forum Young Global Leaders gathering and got to spend time with fellow YGLer **danah boyd**, a researcher at Microsoft who shares this point point of view and articulates the reasoning behind it well: http://www.zephoria.org/thoughts/archives/2010/08/26/regulating-the-use-of-social-media-data.html

In my presentations for the past several years I have been reminding the audiences I speak to about the many reasons that people have to not link all their activities online together and why they have concerns about their dignity being respected. One lens to consider this through is what information can be inferred from one's geo-location log. Are the inferences that can be derived from the data ones that should be made by the collectors of this data? What rights do people have to know, control and correct assumptions that are being made about them via these data streams? What are the appropriate uses of this data?

- **Religious Affiliation.** Do they travel to a mosque most Fridays, a Synagogue on Saturday or Church on Sunday OR perhaps they are witches who gather in large rituals on the beach for the Solstice and Equinox?
- **Ethnic/Racial Identity.** People make choices about how they choose to present their ethnic identity. When we travel about the physical world we can't not show the color of our skin or the shape of our facial features. Online we don't have to reveal these and it should be our freedom not to do so.
- **Goofy Hobbies.** Did you travel to another city for the board gaming convention, or perhaps a show for your favorite type of animal – ferrets – or perhaps you go off the woods dressed as 15th century lords and ladies with the Society for Creative Anachronism.
- **Gender and Sexual Identity.** Do they go to gay bars on Friday night? Maybe a foot fetish party? Perhaps even have made a gender transition or are living their life partly between gender roles. Or maybe just choosing to have a different gender identity for economic purposes. A great example is a woman who spent two years growing a business as a very successful copy editor named James Chartrand. She had tried to get the same jobs when she applied for them as a woman and was rejected so in order to feed her family she took up this pseudonym and became successful. You can read her story in Why James Chartrand Wears Women's Underpants http://www.copyblogger.com/james-chartrand-underpants/
- **Medical or Mental Health Issues.** Are they visiting a particular type of doctor's office regularly and how are assumptions made about why this may or may not be being done made. Many types of illness have social stigma attached and allowing people to keep this to themselves is important so that people actually get help for issues that arise in these realms and that they are not having to explain family issues if they don't want to.
- **Political Speech and Protest.** You've seen photos from the March on Washington where Martin Luther King gave his *I have a Dream* speech. Today there are active protests around the world. People participating in them are putting their lives at risk by doing so. Others who are involved in the Occupy Wall Street or Tea Party movements may not want their work colleagues or bosses to know about their activities. We all get and agree that the right to a secret ballot is fundamental to our democracy. The right to free speech and ability to be present at protest without your activity being tracked must also be fundamental.
- **Exploration of Identity.** When one is young can different aspects one's self or interests be explored in a way that the explorations are not all linked together? If young people can't have the freedom to try on different identities, explore new things, will they reach their potential? Discovering yourself is central to the pursuit of happiness, enabled in a free society.

I think a core value that must be a the heart of this emerging ecosystem to survive is a deep respect for people's human dignity and, with this, their right to make choices about how they are seen in digital spaces.

# Editorial

## By Kelly Mackin

A former Nazi SS Commando, Heinrich Boere, hid out for more than half a century before he was discovered living under an assumed name in Germany. After he was tried, he ended up living in a German prison hospital. The story was that he was later secretly videotaped by two German journalists readily admitting the atrocities he committed. Although this seems like a standard investigative journalism story, this time there was a catch: Boere complained about the violation of his privacy and the two reporters were prosecuted in Germany for violations of Europe's privacy law.

### Press Freedom is Inseparable from Political Freedom

It's a cliché to speak about "freedom of the press" in Western countries and certainly no honest government would be possible without it. But should privacy laws trump freedom of the press? Conversely, are members of the media "above the law" with respect to collecting and investigating stories? The trail of journalist bodies world-wide is stark testimony to the dangers of real journalistic research. But does such an important function need to be supported by some latitude in obtaining evidence to support a story?

### Journalism is not Entertainment

Here in the US, there is a long-established body of law that says that journalists have to obey the law while practicing their craft. But it is possible that privacy laws could make it more dangerous for the press to investigate situations in pursuit of a story? The framers of the US Constitution could have placed press freedom under Freedom of Speech, but in fact they thought it was so important that they created a discrete right in the First Amendment. The central component of a true journalistic act is not publishing but the creation of the story itself. In other words, the primary research and evidence gathering that journalists do is what Freedom of the Press is all about. Without primary data to drive truth-telling, journalism becomes a form of entertainment or propaganda.

### Carve out Exceptions?

While we move headlong into a global framework for privacy and end user control. It's important that we also remember that there are other rights and freedoms that need to be protected as well. It would be truly unfortunate if in search of privacy we inadvertently undermined the central role of a "free press" in pursuit of research and evidence for a story. Or in the case of Germany, inadvertently give a state a method to criminalize the core function of a free press.

From the perspective of the individual, he believed that he had a right to his privacy. From the perspective of the journalists, they were looking to find an exciting story that would advance their careers. From the perspective of the prosecutor, he might have wanted to put the past behind Germany, or he might believe that privacy has to apply to everyone. It was dishonest for the journalists to have taped the man. That much, all will probably agree upon.

It would have been much better for all concerned if the reporters in question had asked for permission to capture video. But the trial of these reporters on what are effectively felony charges could promote suppression of reportage in the guise of protecting privacy. That's a scary prospect indeed in other cases where powerful interests intersect those of the state.

At its core, this whole topic is also about fairness. While it's not popular to say so, even a darkly wrought human like Herr Boerr deserves to be treated the way that we ourselves would like to be treated not because of what it says about him but rather what it says about us. To do anything else portends to descend us into savagery. While in the U.S. reporters and paparazzi engage in this kind of activity all the time, it's daunting to either witness press misconduct *or to ask anyone to limit or regulate it.* Press freedom is all too often an ugly thing to behold however one looks at it. The framers of the American Constitution knew how vicious the press were before and after the founding of the Republic, having suffered its slings and arrows and its psychic wounds. It is not a new phenomenon. But they correctly knew that the light of day was the best insurance for general human rights to be respected and freedom to remain preserved.

In our efforts to build and construct systems for the promotion of end user control and privacy, I hope that we bear close attention to other rights in our systems and standards if the ideals of Western culture are not to be diminished in the push for privacy and end user control.