# The Information Sharing Report

**Version:** Work Group Report.v3

**Date**: 2010-12-06

**Editors**: Joe Andrieu, Judi Clark

**Contributors:** This document is a report of the Kantara Initiative's Information Sharing Work Group based on a comprehensive literature review, research and report by Mark Lizar (mark@smartspecies.com), with contributions from Joe Andrieu (joe@switchbook.com), Judi Clark (coach@digitalidcoach.com), and Iain Henderson (iain.henderson@mydex.org). Special thanks also to Eve Maler (eve@xmlgrrl.com) for her contributions.

**Status**: This document is a Kantara Initiative Work Group Report, and has been approved by the Information Sharing Work Group, for submission to the Leadership Council.

**URL**: This report may be found online at http://kantarainitiative.org/confluence/display/infosharing/Information+Sharing+Report

**Abstract:** This report examines the value of information sharing, where individuals voluntarily provide information to service providers, typically in exchange for enhanced services. Shared information can be information created or curated by the disclosing party—it may or may not necessarily be about the disclosing individual. When shared information contains personally identifiable information (PII), it comes under strict protection and scrutiny. This report aims to describe the emerging information sharing phenomenon, illustrate its challenges, discuss working examples and provide recommendations to further research and development.

**Filename:** Information+Sharing+Report

## Notice

# Table of Contents

**Information Sharing** ..... **5**
*Introduction: The Information Sharing Work Group* ..... *5*
*Overview* ..... *5*
*The Information Industry* ..... *7*
*The Rise of Information Sharing* ..... *8*
*The Value of Personal Information* ..... *10*
*Conceptual Models and Technical Approaches* ..... *13*
*Vendor Relationship Management (VRM)* ..... *14*
*User-Driven Services* ..... *15*
*Volunteered Personal Information* ..... *15*
*Customer-Supplier Engagement Framework* ..... *16*
*User-Managed Access (UMA)* ..... *17*
**Challenges** ..... **20**
*Privacy and Contextual Integrity* ..... *20*
*Trust* ..... *21*
*Risks* ..... *23*
*Regulation* ..... *25*
*Regulatory Calls for Participation* ..... *27*
**Next Steps** ..... **29**
*Modeling Solutions* ..... *29*
*Deploying Systems* ..... *29*
*Standard Information Sharing Agreement* ..... *29*
*Information Sharing Trust Framework* ..... *29*
*Interoperability & Standards* ..... *29*
*Other Organizations* ..... *29*
**Support** ..... **30**
**References** ..... **31**
**Appendix A: IS Organizations and Initiatives** ..... **37**
*Article 29 Working Party* ..... *37*
*DataPortability Project* ..... *37*
*EID - STORK* ..... *37*
*EnCoRe (Ensuring Consent and Revocation)* ..... *37*

*EUROPRISE* ..... *37*
*FIDIS (Future of Identity in the Information Society)* ..... *37*
*ISOC (Internet Society)* ..... *37*
*ISTPA (International Security Trust and Privacy Alliance)* ..... *37*
*OECD* ..... *38*
*OITF (Open Identity Trust Framework)* ..... *38*
*PrimeLife* ..... *38*
*Project VRM* ..... *38*
*TAS* ..... *38*
*VOME* ..... *38*
*WC3 (World Wide Web Consortium)* ..... *38*
**Revision History ..... 39**

# Information Sharing

## *Introduction: The Information Sharing Work Group*

The Information Sharing Work Group[1] (ISWG) at the Kantara Initiative[2] seeks to enable sharing of information by individuals who grant specific permissions.

This sharing should fuel a new class of applications that use dynamically provided data to automatically personalize services. Our contention is that when individuals are able to set usage policy for information they give to service providers, individuals will share higher quality and more sensitive information, more frequently. Also, by being able to use a canonical source for commonly requested information, the quality and efficient use of that information is likely to improve.

We hope to increase the rate and quality of information sharing by making it easier to share in a secure manner and increasing the trust that individuals have in information sharing. Also we hope to encourage service providers and other companies to engage in information sharing using trustworthy practices.

## *Overview*

This report examines the value of information sharing by individuals, who provide information to service providers, typically in exchange for some added value like enhanced services. For example: giving a Search engine your GPS location to enable local search, telling a service your birthday so they can provide birthday reminders to your friends, or simply publishing a status update or a blog article so an online service can publish it to the world.

Shared information can be created or curated by a disclosing party—it may or may not necessarily be about the disclosing individual. This kind of information drives services like Flickr, YouTube, and Wikipedia as well as blogs and status updates at Facebook and Twitter.

When shared information contains personally identifiable information (PII), it comes under strict legal protection and scrutiny. Sometimes it contains nearly meaningless trivia, such as queries entered at a search engine. However, the aggregation of seemingly innocuous information can reveal private details presumed by the searcher to be safe from public eyes.[3] Because there is a relationship between

[1] The information Sharing Work Group is an effort hosted by the Kantara Initiative. The Charter can be found at http://kantarainitiative.org/confluence/display/infosharing/Charter.

[2] Kantara Initiative (formerly Liberty Alliance) is a pioneering community focused on the development of global recommendations in identity management.

[3] In 2006, AOL released millions of search queries for over 600,000 AOL users to academic researchers, believing they had appropriately "anonymized" the data. Reporters from the New York

shared information and personal identity, our work in information sharing is intimately tied to recent advances in identity and data management architectures.

This report aims to describe the emerging information sharing phenomenon, illustrate its challenges, discuss working examples and provide recommendations for further research and development.

Information sharing is a global activity. Today, 26.6% of the world's population is online (Miniwatts Marketing Group, 2010), and interacting with many different service providers. From this online activity, the global information base will double every 11 hours in 2010. (IBM, 2006) A significant portion of this data is shared and provided by individuals. (Nielson, 2010)

As a result, detailed profiles and collections of personal information become available in significant volume for analysis and action by anyone willing to pay the going price. Trading of personal information poses risks to individuals, such as when a person's financial or personal world is violated by fraud, identity theft, or other harms. This digital information sharing is challenging societal notions of privacy and information control as intimate profiles are commoditized and stored for unknowable future uses. The consequences of this vast personal data sphere—which is essentially outside the control of individuals today—are not yet clearly understood.

Identity is inherently tied to information sharing. Even when individual bits of information appear to be suitably "anonymous," they can in aggregate become dangerously revealing. Andrew Churchill aptly explains that, "[p]rivacy and identity are often grouped together as a single issue by virtue of information needing to be identifiable and associated with an individual for it to be a privacy concern." (Churchill, 2009:131)

Our research indicates that individuals and companies would benefit from individuals having greater control of their information sharing relationships. Greater control by the individual can reduce the risks inherent in using online services. This report discusses individual-controlled information sharing, focusing on voluntary person-to-organization sharing.

Times were able to de-anonymize the data and identify specific individuals from their presumed anonymous Search history. (Barbaro and Zeller 2006)

## *The Information Industry*

The information industry[4] is going through rapid evolution as the Internet transforms personal, corporate, and governmental information systems. A significant, recent part of that evolution is the rapid growth of proactive sharing of information by individuals using services like Facebook, Twitter, YouTube, Foursquare, Blogger, and Google.

During the industrial age, information was mostly centralized in proprietary databases and used to manage large public and private sector organizations. It made sense that organization-centric information policies were the norm. Organizations were the ones burdened with large service infrastructures to manage. To protected that investment in information technology, organizations developed policies to facilitate commerce and reduce transaction friction, e.g., Terms of Service Agreements (TOS or TOSA), Privacy Policies (PP), and Acceptable Use Polices (AUP). These were designed to minimize risk and liability and maximize the potential value of information to the organization.

In the beginning of this era of centralized information systems, a company's data was a core proprietary asset, built as a unique competitive advantage through the company's own efforts at data gathering and analytics. In the 1980s, companies in large numbers began purchasing data from outside vendors to use in their internal systems, especially Marketing Information Systems for targeting and tracking potential customers. This led to a rapid rise of the multi-billion dollar consumer information industry.

Customer Relationship Management (CRM) systems gather and analyze information about customers in support of advertising and marketing services. CRM is based on finding, acquiring, welcoming, developing and retaining a customer relationship, balanced with how much revenue/profit comes from it. The global market for CRM applications and business services is currently estimated to be close to a $15 billion a year industry. (Lauchlin, 2009) However, Henderson (2009) points out that traditional CRM manages “relationships” that are almost entirely one-sided. Only one of the parties—the supplier—has sophisticated relationship management tools in place. The power they generate is often used to extract value from the buyer rather than to provide mutually beneficial increases in value for both buyer and supplier.

The Internet and the World Wide Web took the information industry from isolated information services built by major organizations to run internal operations, to a

[4] Information industry as we mean it includes information services, database companies, analytics firms, online advertisers and advertising services, marketing firms and networks, customer relationship management software and services, and those explicitly involved in the management of information.

widespread internetwork of diverse service providers facilitating business-to-business, business-to-consumer, and consumer-to-consumer interactions. Corporations and governments no longer use information technology just to manage their own activities; they use it to reach out to their constituents and stakeholders, to provide services external to the organization.

Corporate and governmental, as well as individual use of internetworked data is predicted to continuously increase. Overall Internet traffic is expected to grow at a compound annual growth rate of 34 percent, and quadruple from 2009 to 2014. In 2014, global IP traffic is expected to reach 767 exabytes[5] per year or 64 exabytes per month. (Cisco, 2010)

## *The Rise of Information Sharing*

The advancements in personal and mobile computing over the last two decades[6] have greatly decentralized the access to, storage of, and use of digital information. In the resulting internetworked digital world, industrial age approaches to information management are rapidly becoming outdated. The old approach limits information sharing, lacks contextual integrity (the intent behind and purpose for sharing the original data), and actively minimizes the understanding individuals need to effectively balance the social, legal and economic risks of their online interactions.

The first generation of services built on shared information focused on "user-generated content" and followed an industrial model: accumulate data or content in a central location, using an organization-centric Terms of Service, then package and redistribute that content in a way that creates value for both users and the company. This is the model of CompuServe and AOL, service providers that ran bulletin boards and discussion groups using the posted conversations of their users, with users actually running the groups. It is also the model of Google, a company that built a searchable index of websites built by others

Another service built on shared information is Wikipedia, which publishes encyclopedic articles written, edited, and maintained by its users. It was searched 375 million times a day in May 2010 (Wikimedia, 2010), illustrating the power of shared, aggregated information, now available to millions of people around the world. Others popular services built on shared information include Google, which received over 2 billion searches a day in 40 different languages, (BBC, 2010) and YouTube, which got more than 2 billion views a day. (YouTube, 2010).

---

[5] 1 Exabyte = 1,048,576 terabytes

[6] Technical advancements in personal and mobile computing include; storage space, computing power, connectivity, mobile devices.

A second generation of services focused on distributing information to individuals' social contacts. These "social networks" or "social media" sites rapidly caught on as people could pick and choose whose information they viewed and who, in turn, got to see their information.

Facebook has emerged as the largest player in this space, with mutually confirmed relationships between "friends" with whom users can share detailed profiles, photos, links, and status updates. Facebook has over 500 million active users who spend over 500 billion minutes per month interacting with over 160 million objects. The average user is connected to 60 pages, groups or events, and creates 70 pieces of content each month. Overall, more than 25 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) are shared each month. (Facebook, 2010)

The third generation of services based on shared information is just now emerging, allowing individuals to share not just with other individuals, but with third-party companies and organizations seeking to provide enhanced online experiences. Facebook is leading in this area as well. Their popular application framework allows companies to offer applications directly within Facebook's service. The service provider recently launched Facebook Connect, which allows third party websites to access user's Facebook identities and friend lists to customize the third party services. As of this report, “two-thirds of comScore’s U.S. Top 100 websites and half of comScore’s Global Top 100 websites have integrated with Facebook.” (Facebook, 2010) There are more than 200 mobile operators in 60 countries working to deploy and promote Facebook mobile products. (Facebook, 2010)

This ability for individuals to proactively share information when they want to has combined with a growing public mistrust of online services' practices to fuel a revolution from company-centric customer relationship management (CRM), to customer-managed interactions. (Watson et al., 2003) This is happening both in private commerce and the public sector as both the United Kingdom and the United States begin to embrace newer distributed and shared identity systems.

In 2009, the Open Identity Exchange (OIX) trust framework[7] was developed for the U.S. General Services Administration (GSA) on behalf of the Identity, Credential, and Access Management (ICAM)[8] industry to support E-Government activities and to leverage industry-based credentials—which citizens already have for other purposes. Such a framework was required in order to ensure these credentials are

[7] OIX Trust Framework. http://openidentityexchange.org/

[8] Identity, Credential, and Access Management (ICAM)_ http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV

trusted by various federal agency websites.[9] (OIX, 2010) The OIX trust framework is now seen as a useful starting point to develop an information sharing infrastructure that enables the extension and use of identity-related data across the Internet.

In the United Kingdom, the pushback against centralized identity management and large inter-connected databases has had a notable impact in the political realm. The recently elected coalition government halted a government-driven national identity scheme, and has launched a Freedom Bill (Number10, 2010) with plans to decommission major centralized database projects. (Anderson et al., 2009) One driver of this trend has been data breaches, large-scale loss of personal data, typically from centralized systems run by a large organizations. The largest data breach in British History was by HM Revenue and Customs, which lost 25 million child benefit records in October 2007. From October 2007 to October 2008 there were an estimated 277 data breaches. This grew to 434 recorded data breaches recorded in the next year from October 2008 to October 2009. (Whitehead, 2009) Many of these high-profile data breaches have degraded perceptions, policies, and economics surrounding information regulation in British society.

## *The Value of Personal Information*

Understanding the value of information sharing is difficult. Quantifying it is even harder. “The value of personal information is determined by how much it takes to relinquish it.” (Solove, 2004) In Solove’s book *The Digital Person*, he described an information industry where the emphasis has been on the organization's ability to gain access to personal information in order to better target direct marketing. Solove’s research revealed that in 2001, direct marketing resulted in 2 trillion dollars in sales in the USA. As a result “due to targeting, direct mail yields $10 in sales for every $1 in costs.” Solove points out that when aggregated, personal information is also valuable because it can be very revealing as combined details paint a more candid picture of an individual than evident from the isolated bits. He further noted, “[t]he aggregation effect severely complicates the individual's ability to ascribe a value to personal information. In addition, the future uses of personal information are so vast and unknown that individuals are unable to make the appropriate valuation.”

Current research in the UK (illustrated in Figure 1) indicates that people have divergent opinions regarding the value of their personal information.

[9] OIX is intended to enable Open Id to be usable with US institutions such as the National Institute of Health (NIH), the National Library of Medicine (NLM), and the Library of Congress (LOC)] to begin accepting OpenID and Microsoft Information Card credentials.

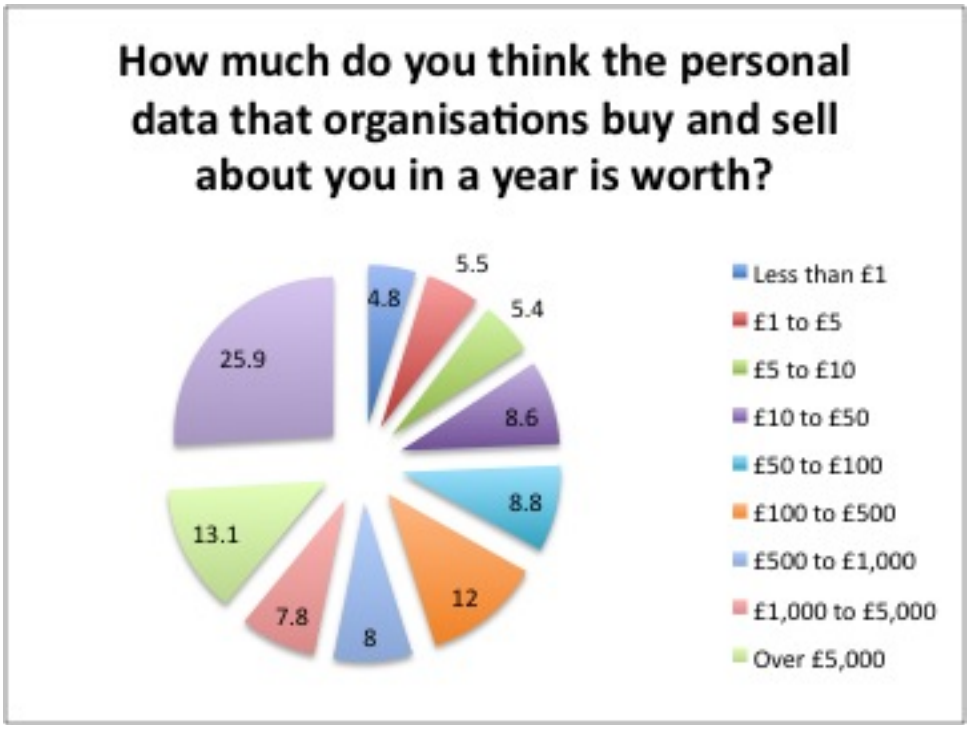



**Figure 1: Guessing the Value of Personal Information** (Mydex, 2010)

Another way to look at the value of personal data is by the business cost it takes to maintain this information. Current estimates are that a data breach costs £64 per record in the UK. (Broersma, 2010) A large organization might easily spend an average of £3 to manage and maintain one record per year. (Henderson, 2009)

One further way to look at the value of personal data is to look beyond the information bought and sold by data brokers to the more immediate, attention-based, personal interest information that can be harvested while people surf the web. Even though traditional web banner advertising is stagnating, behavioral and situation-based advertising is growing rapidly. For example, Google's profits are up 37 percent in the first quarter of 2010. (Liedtke, 2010) The company has earned nearly $2 billion in the first quarter and is considered to be the leading company in what is expected to be a $24 billion a year on-line advertising industry. (Lee, 2010)

Personal information is now being aggregated and mined on a massive scale to target advertising and direct marketing efforts. Our demographics are driving advertising, recommendation systems, and Internet behavior. (BBC, 2010) This is not what most people initially expected when they began using Internet-based services. As a result, regulators are becoming increasingly aware of potential abuse and exploitation of personal information shared online.

The value of an individual's shared information[10] (depicted in Figure 3) will increase significantly over the next ten years, according to Mitchell, Brandt, et al. (2009). Their graph illustrates the market size of four categories of shared information in the UK:

1. My Views and Feelings
2. What I want
3. What I want to find out
4. Who I am

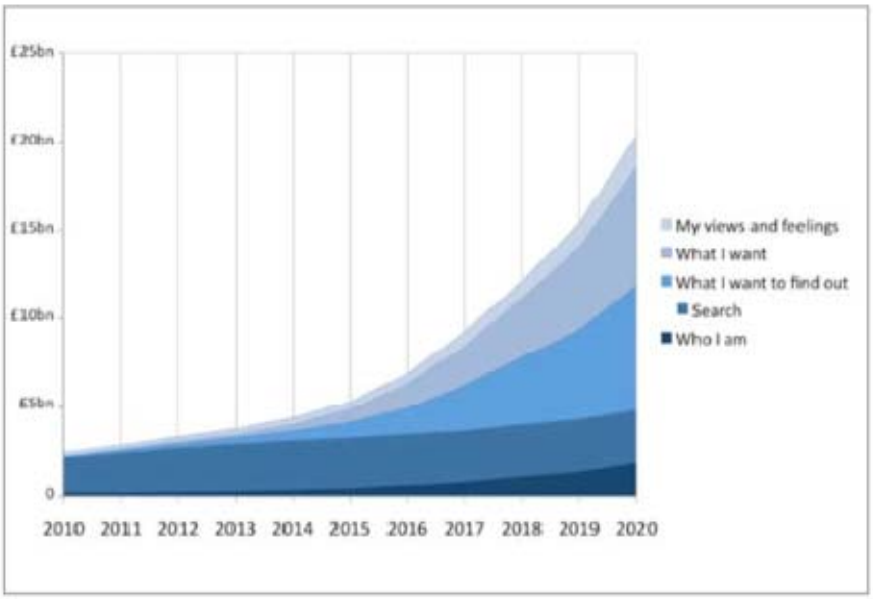



**Figure 3. Growth of value in Shared Information**:
This figure depicts the estimated value of shared information in the UK from 2010-2020.

Much of the value is expected to be created in situations where customers manage their own information sharing with suppliers. In turn, suppliers allow customers to directly manage various interactions. Mitchell suggests that specific types of information are most suited to the volunteered information sharing approach between enterprise and individuals (Mitchell, Brandt, et al., 2009):

- **Factual updates** (e.g. I've changed address/email address, I'm reading War and Peace)
- **Change of Circumstance** (e.g. we're getting married, I've now got 3 points on my license)

[10] Referred to as Volunteered Personal Information (VPI) in the report

- **My Location** (e.g. I'm in the Wellcome Collection café)
- **Factual queries** (e.g. I don't understand my bill, where's my order)
- **Online searches** (e.g. this is what I am interested in right now)
- **Orders** (e.g. I would like to buy this, please)
- **Specifications** (e.g. please give me these features, functions etc)
- **Complaints** (e.g. this does not work to spec, can you help?)
- **Suggestions** (e.g. why don't you make X?)
- **User generated content** (e.g. personal, creative expression)
- **Views, reviews and opinions** (e.g. I tried that, and in my experience…)
- **Shared experiences** (e.g. I had a similar problem, I know how you feel)
- **Peer advice** (e.g. I had a similar problem, what I learned was)
- **If only...** (e.g. what I would really like is X, but nobody is offering it)
- **Future plans and intentions** (e.g. I plan to buy a car in the next three months)
- **Expressions of interest** (e.g. I am interested in golf but not scuba diving)
- **Preferences** (e.g. I don't like green but I do like blue)
- **Questions** (e.g. I don't understand! But what about?)
- **But what if...** (e.g. what will happen if I do X or if I do Y)
- **Permissions** (e.g. I am happy for A but not B to access my data, for these purposes)

The true value of these information types is yet to be fully realized by individuals, governments and organizations.

## *Conceptual Models and Technical Approaches*

There are several different conceptual models for implementing information sharing practices. Vendor Relationship Management encourages development of tools of both customer independence and engagement. User-Driven Services outlines ten characteristics that increase the value of a service by increasing individual authority and control. Volunteered Personal Information focuses on the source and use of different data, especially that provided directly by individuals. The Customer-Supplier Engagement Framework is a model of the entire relationship involved in every transaction. User-Managed Access specifies a technical mechanism for giving individuals the ability to directly manage access to hosted data and services. Together, these models outline a new architecture for online services, one with the

individual at the center as the point of integration, as the source for both data origination and control.

## Vendor Relationship Management (VRM)

The concept of Vendor Relationship Management, or VRM, was proposed by Doc Searls, community leader of ProjectVRM.[11] This community is actively driving a conversation around customer-managed interactions. VRM is the conceptual reciprocal to Customer Relationship Management (CRM). In contrast to enterprise software that helps large organizations make more money from "consumers," VRM hopes to build tools that help individuals get more out of their relationships with vendors. (ProjectVRM, 2010)

The community supporting ProjectVRM aims to "provide customers with both independence from vendors and better ways of engaging with vendors. […] Customers will also be involved, as fully empowered participants, rather than as captive followers." (Searls, 2009) Toward that end, ProjectVRM leader Doc Searls has proposed an emergent class of businesses that he refers to as "Fourth Party Services" (Searls, 2009). These services work on behalf of individuals to support and facilitate their relationships with vendors.

ProjectVRM has proposed the development of a Personal Request for Proposals (pRFP). Based on the practice of publishing Requests for Proposals (RFP) for procuring big-ticket items or major contract work, the pRFP is seen as an open platform for individuals to publish their intent to purchase a specific item, or even a shopping list of items. Rather than directing that pRFP to a single company, it would go through one or more pRFP brokers[12] to any number of interested vendors. Each pRFP broker is acting as a Fourth Party Service[13] on behalf of the requesting individual, where the individual has complete control over who is allowed to view the pRFP and how the pRFP process proceeds. (ProjectVRM Wiki, 2009)

Also emerging from the VRM conversation is the development of a Personal Data Store (PDS), a virtually distributable collection of information controlled by an individual and accessible by vendors according to permissions set by that person. A number of services already act as limited personal data stores, including Flickr, blogs, and IMAP and POP mail services. However, few of these services give users

[11] ProjectVRM is run by Doc Searls, a fellow at the Harvard University Berkman Center for Internet & Society. "By providing customers (and users) with their own tools for managing relationships with vendors, Searls sees VRM as "a way to fulfill one of the promises of The Cluetrain Manifesto" — the widely-cited website and book co-written by Searls in 1999. (Levine, Locke, et al. 1999)

[12] Including the possibility of the individual acting as their own pRFP broker by running their own pRFP broker service.

[13] Doc describes fourth party services here: http://blogs.law.harvard.edu/vrm/2009/04/12/vrm-and-the-four-party-system/

the fine-grained control and robust authorization management that is required for users to effectively publish something like a pRFP. The full potential of the personal data store requires a user-controlled identity-moderated data store, third party claims validators, legally binding access rights agreements, and open standards and protocols for communications between vendors and personal data stores. (Andrieu, 2007a)

### User-Driven Services

Businesses and services of all types are becoming more and more "user-driven," giving users greater authority and control in order to create more value for both individuals and their vendors. (Andrieu, 2009) Andrieu presents ten characteristics of User-Driven Services as a roadmap for companies seeking to leverage shared information effectively:

1. Impulse from the User
2. Control
3. Transparency
4. Data Portability
5. Service Endpoint Portability
6. Self Hosting
7. User Generativity
8. Improvability
9. Self-managed Identity
10. Duty of Care

Services with these characteristics, Andrieu argues, will be best able to leverage emerging information sharing architecture by building their services with the user as "the point of integration." This architecture puts shared information under the individual's control, yet is seamlessly accessible by authorized vendors. This enables a personal data store to fuel user-driven services in the cloud. (Andrieu, 2007b)

Andrieu also proposes that in order to realize the potential of information sharing, regulators and privacy advocates should direct their attention away from complex and distracting debates about data ownership, and toward a contractual information sharing agreement entered into at the point of sharing. He argues that such an agreement would bootstrap a regime for managing shared information independent of arguments about ownership. (Andrieu, 2010)

### Volunteered Personal Information

The *Personal Data Eco-System* describes five types of personal data and how information sharing could evolve over time. (Henderson, 2009)

1. **My data** (mine and only mine)
2. **Your data** (yours, and only yours – typically a supplying organization)
3. **Our data** (jointly owned)
    a. The data I brought to the relationship

   b. The data you brought to the relationship
   c. The data we co-create within the relationship
4. **Their data** (the data aggregators, with no direct relationship to the individual)
5. **Everybody's data** (public domain data, e.g. www.data.gov)

Henderson illustrates the commercial flows of customer-related information:

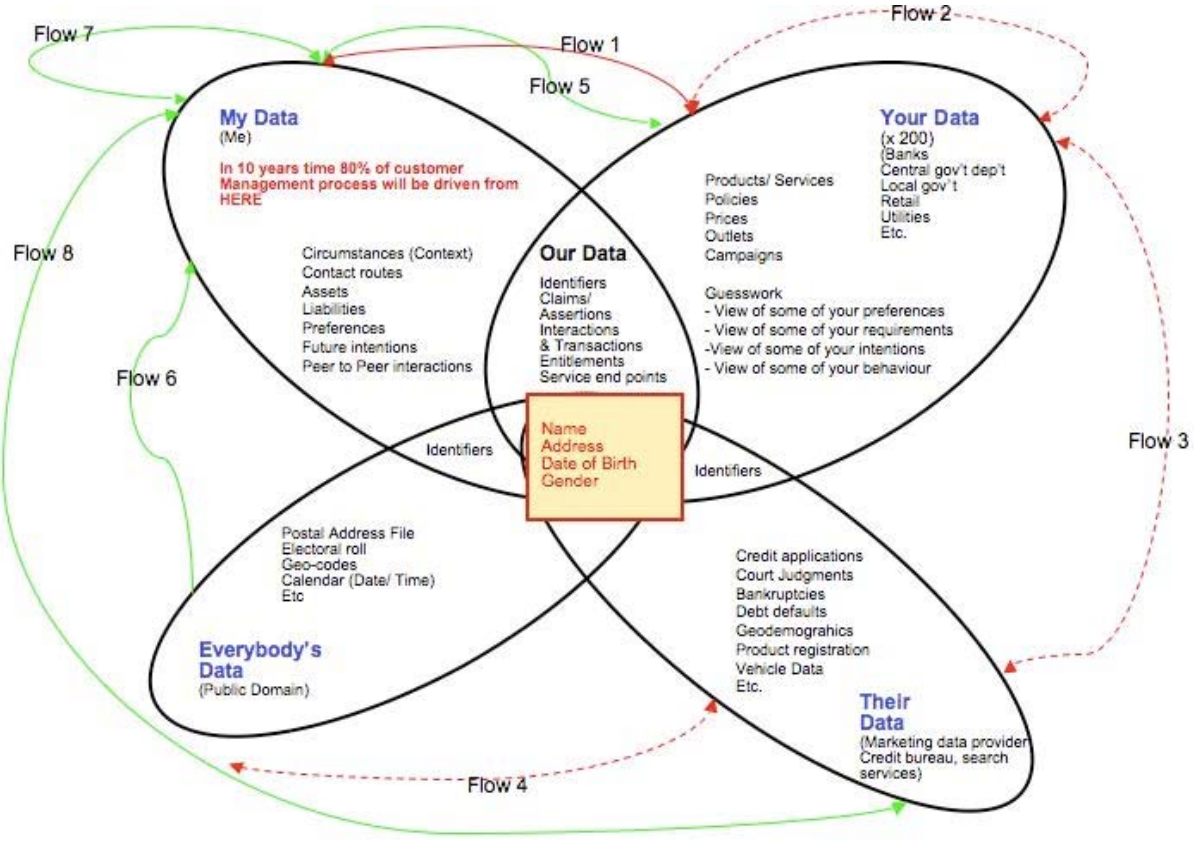



**Figure 2: Data Relationships**
Existing and future data flows:
Red lines = current flows, green lines = emergent flows

"My Data" has the key distinguishing feature that it can only be released under the power and control set by the individual—either overtly or derivable through positive action. "[T]he individual and 'My Data' can become the dominant source of information fed into customer management processes (e.g. buying intentions, verified changes of circumstance), and in doing so will eliminate vast amounts of guesswork and waste." (Henderson, 2009)

## Customer-Supplier Engagement Framework

In the Information Sharing Work Group, the 'Customer-Supplier Engagement Framework' (ISWG, 2009) maps 11 high level stages in customer-supplier relationships. The following diagram illustrates current information flows, where new and/or improved flows will be of use, and what capabilities are required to

enable these flows. This reverse flow (customer-to-business) of information can then be used to develop generic (Internet scale) processes like the pRFP.

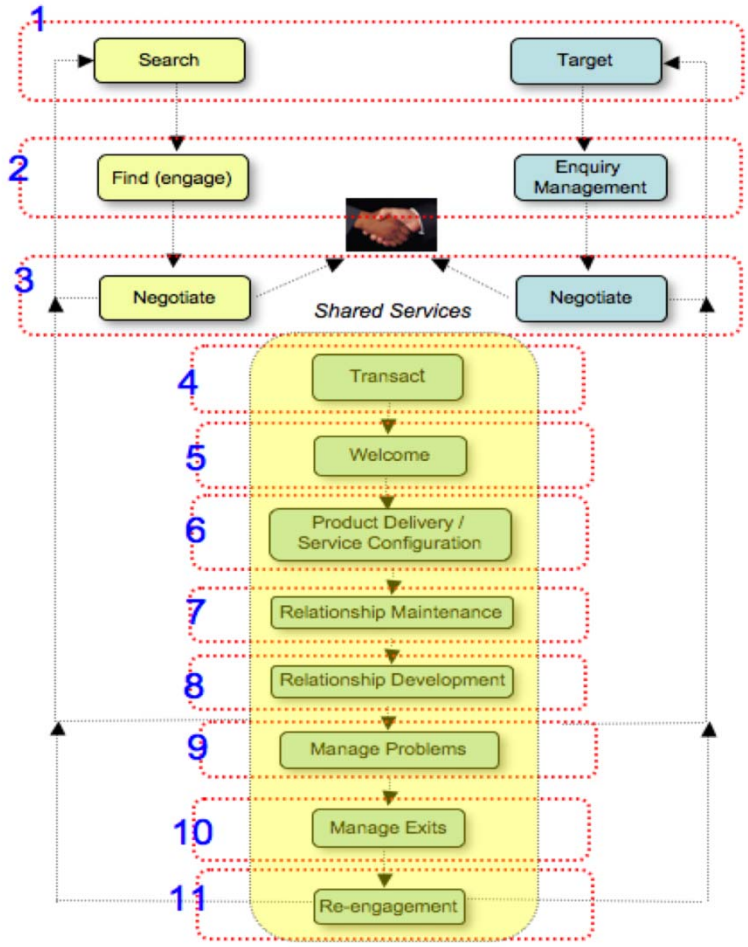



**Figure 6: ISWG's Customer-Supplier Engagement Framework**

## User-Managed Access (UMA)

The Kantara Initiative's User-Managed Access (UMA) Work Group is developing specifications that let an individual control the authorization of data sharing and service access. (Maler 2010a) The UMA Work Group has designed an information sharing protocol based on OAuth 2.0 (a core protocol for authorization management) that offers controlled, granular access to information hosted online. It is also facilitating interoperable implementations of the specification.

User-Managed Access (UMA) involves the following entities:

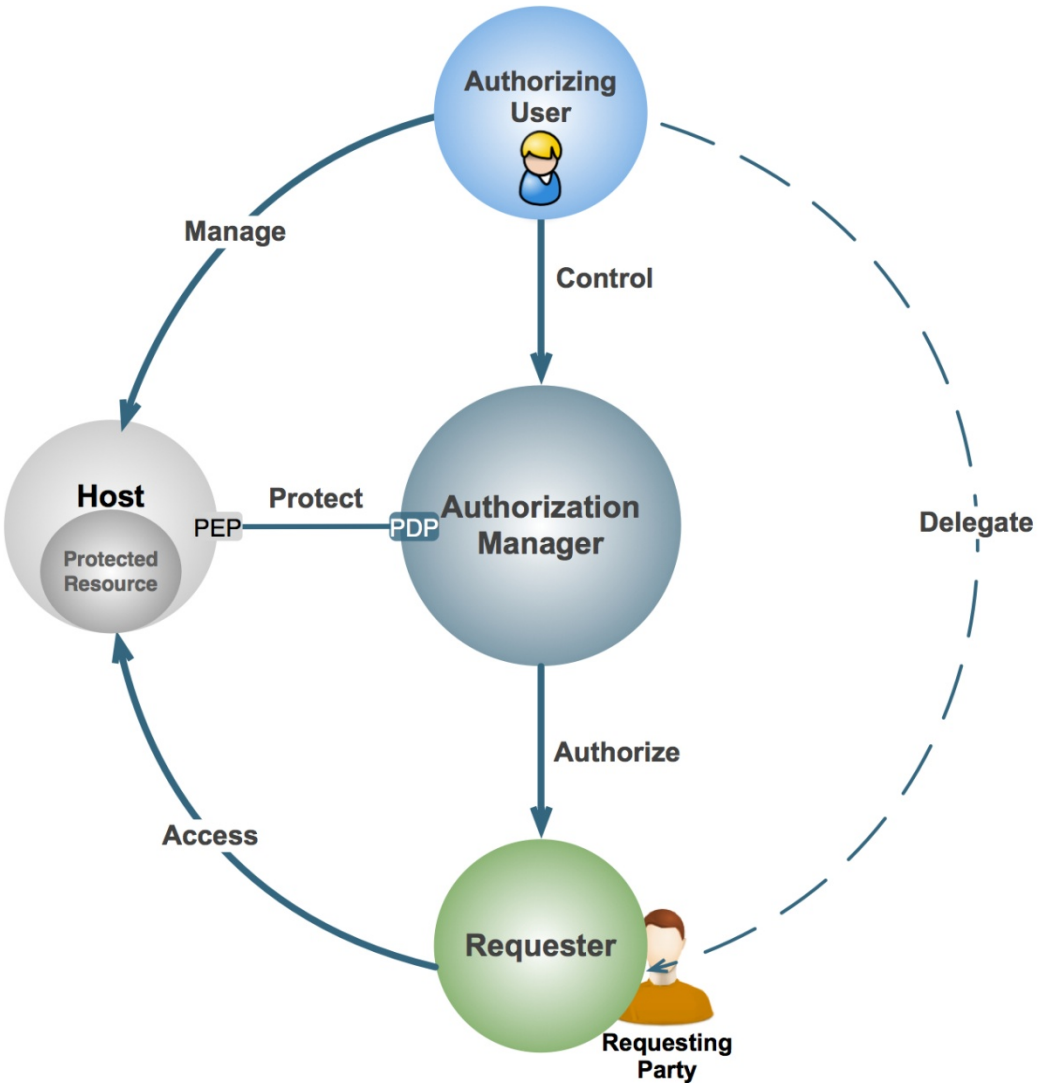



**Figure 7: User-Managed Access**

For example, a web user (authorizing user) can authorize a web app (requester) to gain one-time or ongoing access to a resource containing his home address stored at a "personal data store" service (host), by telling the host to act on access decisions made by his authorization decision-making service (authorization manager).

The requesting party might be an e-commerce company whose site is acting on behalf of the user himself to assist in arranging shipment of a purchased item, or a friend who is using an online address book service to collect addresses, or a survey company that uses an online service to compile population demographics. (Maler, 2010b)

The UMA protocol supports the policy-driven ability of an Authorization Manager to demand "claims" from a Requesting Party before authorization is granted. The claims may be self-asserted or third-party-asserted, and may represent statements of fact (such as "is over the age of 18") or promissory statements (such as "agrees to adhere to the authorizing user's privacy and data portability policy").

# Challenges

Several key challenges must be addressed to effectively realize the promise of Information Sharing as envisioned in this report:

1. Privacy and Contextual Integrity: How does privacy work in the digital realm?

2. Trust: How do we establish and deliver on the trust required for people to share information?

3. Risks: What are the risks we must address?

4. Regulation: How do current regulations affect information sharing and how should we regulate this domain moving forward?

## *Privacy and Contextual Integrity*

Management of shared information means that we must also manage the contexts in which the information is released and propagated. Traditionally, individuals have managed context sensitive disclosure automatically, by moderating what they say, where they say it, and to whom they say it. Privacy violations occur when information leaks from one context to another. For example, Alice tells her doctor Bob about an embarrassing problem and he tells his wife, Carol who happens to know Alice from the Parent Teacher Association (PTA): the information has leaked from the doctor-patient context to the PTA context, violating Alice's privacy.

Acquisti points out that privacy is inherently a social construct:

> Privacy as a social space is comprised of visible discretion for society to manage the use of personal and sensitive information. (Acquisti, 2004 p.2)

The challenge is to enable the individual to control the context of information usage in the broader digital realm—where copying and distribution isn't just commonplace, it is innate to the medium itself. (Kelly, 2008)

> A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes.' The basis of privacy as contextual integrity is based on two "informational norms"--norms that 'govern these contexts of social life,' defined as norms of 'appropriateness' and 'distribution'. (Nissenbaum, 2004:p.106)

Ian Glazer and Bob Blakley (2009) of The Burton Group offer a principled approach to the development of information sharing practices for organizations. These principles begin with the understanding that privacy is fundamentally contextual. Any question about privacy must be understood in the context of:

- The starting assumptions and principles of the parties
- The relationship between the parties
- The interaction between the parties where private information is shared

- The domain (e.g., sector, nation, etc.) in which the parties are interacting
- The societal norms to which the parties adhere (Glazer & Blakley, 2009:p.31)

For organizations, this approach will allow people to properly manage their expectations and understandings about the use of shared information.

## *Trust*

Trust is "a leap of faith" (Cofta 2007), and as such it is clearly evident in our willingness to use online services without verifying the safety of doing so. Only 20% of Internet users say they read privacy statements, if provided, "most of the time." Only 5% have read a policy again for changes. (TRUSTe, 2006) And yet, "60% of online shoppers abandon their carts at some point during their shopping experience, mostly due to fear of identity theft, and almost half (44%) say they're less likely than they were just a year ago to trust a Web merchant with personal data." (Maier, 2009) This contrast of implicit trust and voiced distrust reveals a confusing mix of wishful thinking and ever-present low grade fear about the abuse of information revealed online.

Seligman (paraphrased in Lewis, 2009) points out that "there is a fundamental difference between *trust in people* (interpersonal relationships) and *confidence in institutions.*"

Interpersonal trust and institutional trust are distinct concepts, each made operational in different ways. (Morrone, Tontoranelli, & Ranuzzi, 2009) Privacy attitudes and behaviors will change according to the level of trust or risk people perceive for the people or institutions with which they are interacting.

In the Trustguide (Lacohée et al., 2006:p.14-15), a qualitative trust research report, the authors found a very low level of trust with information communication technologies (ICT) from the outset.

> [A]s more data is gathered and stored electronically—particularly in central databases—and the more they use ICT-mediated services, the more vulnerable they feel." The perceived risk of involvement with ICT increases with use, revealing that "the perceived risks and associated decision making processes that users are prepared to undertake in order to avail themselves of the advantages that technological advances afford are worthy of a good deal more attention." Research participants "commonly referred to 'risk' rather than 'trust' when describing their ICT mediated experiences. (Lacohée et al., 2006)

Perhaps a degree of trust in current online activities should be attributed to trust in the Internet as an institution: everyone is doing it, it is well established, the system as a whole must be working. For whatever reason, millions of people trust online service providers with their personal information every day, despite continued concerns over the risks of doing so.

> [i]f a trusting act was based upon calculation of expected outcomes or on the rational expectation of a quantified outcome, this would not be an act of trust at all but an act

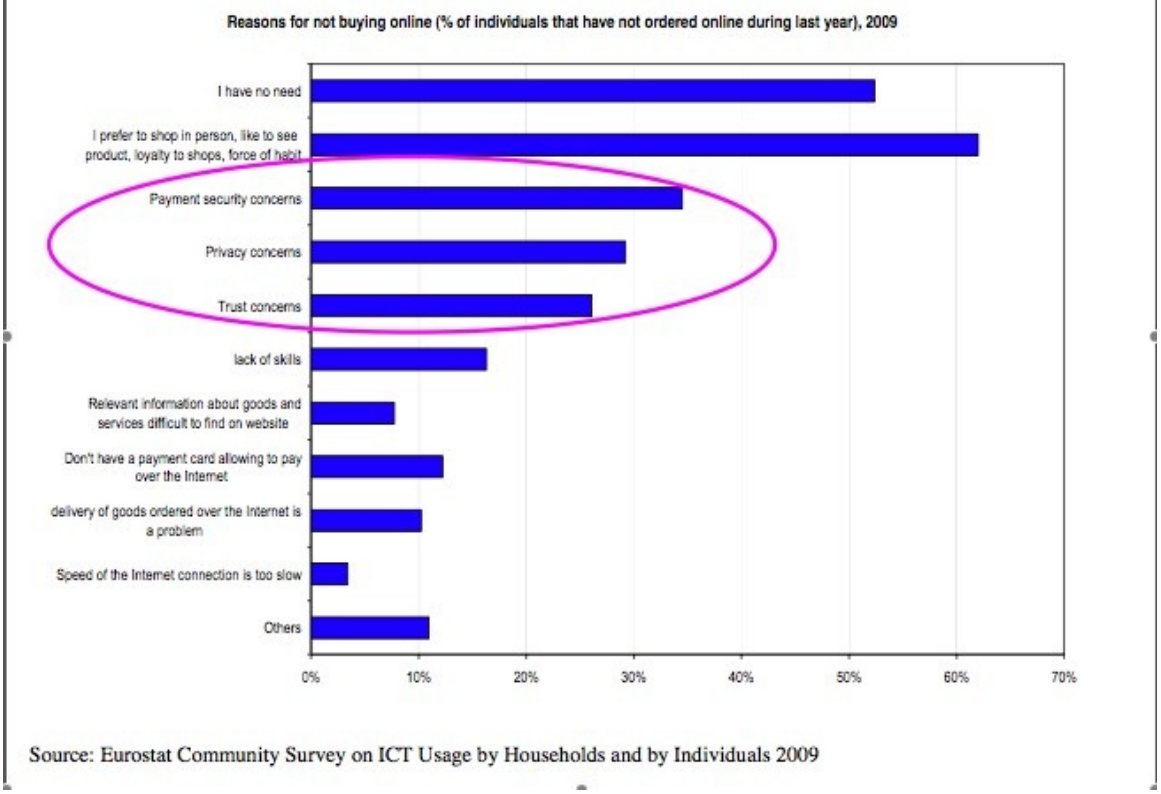
> based on confidence. This would be based upon the idea of confidence in the existence of a system that delivered what it promised. The suspension of reciprocal calculation is precisely what defines trusting relationships. (Seligman, 1997)

In a Europe-wide comparative privacy survey about consumer concern over data security, the authors found that:

> [A] large majority of those respondents who were Internet users reasoned that data transmission over the Internet was not sufficiently secure (82%), while only 15% of respondents trusted data security transfers over the Internet. (The Gallop Organization, 2008)

This lack of trust in the online environment is viewed by some as seriously hampering the development of Europe's online economy. The three of the top five reasons among people who did not order goods or services online in 2009 were: payment security concerns, privacy concerns, and trust concerns (Figure 3, below). The European data protection regulatory framework aims to modernize all relevant legal instruments to meet the challenges of globalization and to create technologically neutral ways of enhancing trust and confidence. (Jaquet-Chiffelle & Buitelaar, 2009:12)

**Figure 3:** Reasons for not buying online (% of individuals who have not ordered online in 2009)




Source: Eurostat Community Survey on ICT Usage by Households and by Individuals 2009

**Figure 5: Reasons for not buying online**

Edgar Whitley, a professor at London School of Economics, notes that, "[I]n recent years there has been growing recognition that providing users with control over their personal data is an important aspect for maintaining trust in an online environment." (Whitley, 2009) Whitley explains, "in an Internet enabled society it is increasingly important to understand how disclosed data is being used and reused, and what can be done to control this further use and reuse." Whitley points out that "consent to the processing of personal data is probably the most important mechanism that currently exists for determining how and when this data can be used."

Cofta points out the inherent link between trust and control:

> Trust and control are interchangeable and in the absence of trust there is control. […] Trust in fact is a deficiency of control that expresses itself as a desire to progress despite the inability to control. ...[W]hile control is reducible to trust, trust cannot be reducible to control." (Cofta 2007)

Revocation of consent introduces a new form of control over personal data that "has not been well studied in the literature or in the practice of informational privacy." (Whitley, 2009) Consideration of consent opens up our understanding of the nature of informational privacy and control, and offers new opportunities (beyond anonymization) for addressing concerns that individuals have about data handling.

However, addressing perceived concerns doesn't necessarily remove the risk of abuse. The Open Identity Trust Framework (OITF) report (Rundle 2010) stated that "it is clearly important to safeguard against ways in which a system with the potential to enable trusted transactions at Internet scale could be abused…" The OITF report concluded:

> "The authors [of the OIX report] want to make it clear that trust frameworks for identity information portend to be so important for the future information society that they warrant extensive scrutiny, participation, and feedback from a wide representation of stake holders." (Rundle 2010:p.14)

Lewis suggests that only discussions using motivation as a starting point can get it right. Regulation and legislation (data protection legislation, for example) or technology-based solutions (identity management solutions) can exacerbate rather than allay fears because they fail to take into account the trust relations underpinning them. (Lewis, 2009)

## *Risks*

In the article *Reflections on Privacy, Identity and Consent in On-line Services,* Louise Bennett (2009) noted that "on the Internet we are all, to some extent, operating both in private and public." She pointed out that consumer engagement

offers value in the form of perceived convenience, discounts, and satisfaction, which people weigh against the perceived risk of using online services.

The Australian Communications and Media Authority (2009) found:

> The type of, and level to which personal information is disclosed is seen to be within an individual's control and a matter of personal choice. More specifically, the decision to disclose personal information is based on an assessment of the benefits that will be afforded by the disclosure of such information, versus the risk inherent in such information being disclosed.
>
> These risks are identified in this report are:
>
> - Risks to personal safety and well being, or the safety of others (particularly children)
> - Risk of identity theft
> - Risk of financial loss/fraud/theft (could include malicious software)
> - Risk of damage to reputation
> - Risk of an invasion of privacy (access to personal information without permission)
> - Risk of exposure to unwanted communications (spam or push marketing) (Australian Communications and Media Authority, 2009:1-2)

*Privacy and Security of Personal Information,* Acquisti (2004) offers an example of how easily identification happens in common information sharing practices.

> In the majority of real life instances the off-line and on-line identities of a same individual are linkable (or, in fact, linked) together because of legacy applications and existing infrastructures. Re-identification or "trail" attacks can expose an otherwise anonymized identity by matching data from different sources. In the Amazon case, I might login with a certain un-identifiable email address and then receive a certain cookie on my computer (two items potentially representing on-line identities). The cookie and the email address could then be linked to my credit card information (the off-line identity) released when I check-out. Now not only Amazon, but also possibly also other third parties may be able to link my on-line behavior to my real identity. (Acquisti 2004:p.3)

Inadvertent personal transparency created by using on-line services is significant, most likely far beyond what most people realize. The level of surveillance people are now under creates un-quantifiable risks:

> Facebook holds and controls more data about the daily lives and social interactions of half a billion people than 20th-century totalitarian governments ever managed to collect about the people they surveilled. (Moglen, 2010)

The Canadian Privacy Commissioner Jennifer Stoddart warns that Facebook exposes people to blackmail. (McNish & El Akkad, 2010) Not only are people vulnerable on Facebook, but recent policy changes that have made personal data more available to companies using Facebook have been implemented overnight and without warning. (Kohnstamm, 2010a) People are not aware of their exposure. Companies

are aggregating information without a defined purpose against Fair Information Practice (FIPS)[14] (BBC, 2010) and in contravention of data protection law. (Kohnstamm, 2010b)

## *Regulation*

Beginning with the Universal Declaration of Rights in 1948, legislation has been evolving globally. Between 1973 and 1988, 18 OECD countries implemented privacy legislation or action. (Bennett, 1992:p.57) In Europe, Directive 94/95, data protection aimed at harmonizing privacy regulation was implemented in the late 1990's (illustrating a mature discourse in information sharing regulation), although today adhering to these regulations continues to present significant challenges.

By its nature, the Internet makes it easy for services to reach across international boundaries, resulting in complicated legal and jurisdictional questions. Dealing with issues of both enforcement and policy, regulators grapple with establishing appropriate doctrine to address this rapidly evolving part of society.

Paul Ohm points out that the concept of "anonymization" underlying much of our regulatory discourse is itself problematic:

> [C]omputer scientists have recently undermined our faith in the privacy-protecting power of anonymization, the name of a technique for protecting the privacy of individuals in large databases by deleting information like names and social security numbers. These scientists have demonstrated they can often 're-identify' or 'de-anonymize' individuals hidden in anonymized data with astonishing ease. By understanding this research, we will realize we have made a mistake, labored beneath a fundamental misunderstanding, which has assured us much less privacy than we have assumed. This mistake pervades nearly every information privacy law, regulation, and debate, yet regulators and legal scholars have paid it scant attention. We must respond to the surprising failure of anonymization, and this Article provides the tools to do so. (Ohm, 2009:1)

Ohm provides a clear example of how technology is currently out-pacing law, and the scope of vulnerabilities that individuals are now exposed to. The potential loss of anonymity in information sharing illustrates a need for regulation and more appropriate governance to administer what was once understood as privacy.

---

[14] Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information -- their "information practices" -- and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely accepted principles concerning fair information practices. (28) Common to all of these documents [hereinafter referred to as "fair information practice codes"] is five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. (Federal Trade Commission, 2007)

The EU research network Future Identity in the Information Society (FIDIS)[15] suggests that practices that are legal for off-line information sharing are useful to guide the development of an online information infrastructure.

> Putting it into a wider context of the fundamental goal of law, which finds its roots in the philosophies of Aristotle, it may be argued that law should seek to inculcate habits of good conduct and should support a social environment which will encourage citizens to pursue worthy goals and to lead valuable lives. Thus law and ethics complement each other. Ethics sets the basic societal interests that law should guarantee. If we extend this principle to the codes of conduct in the digital world, it is easiest to take as a starting point the principle of "what applies off-line should apply online." (Jaquet-Chiffelle & Buitelaar, 2009)

Carrying norms from offline to online allows people to anticipate "normal" behavior, and, when normalcy is clearly defined, enables greater trust in online services and related information sharing. Although the Internet is perceived by some as a cyberspace of its own, independent of earthly geography, "an electronic place and sovereignty" (Zekos 2007), the individual users, the service providers, and the hardware itself all exist in well-defined geographic jurisdictions. Unfortunately, in any given interaction, numerous jurisdictions may apply, making it difficult for regulators and enforcement agencies to understand the best way to oversee and govern online activity.

With interactive services, one can, in theory, trace the communications path "in real-time" through the various jurisdictions. However, in many information sharing scenarios, the information is created or provided in one jurisdiction to a service provider who may not share that jurisdiction, and later distributed to other service providers in potentially new jurisdictions. Furthermore, the information may be transformed or aggregated en route, making the provenance—and hence originating jurisdiction—difficult or impossible to discern. This cross-jurisdictional nature of information sharing has led to numerous jurisdictional disputes that "straddle[] the boundaries between public and private law, criminal and civil law." (Kuner, 2009) The result is myriad efforts in multiple jurisdictions as each interested party attempts to address their own needs.

In 2010 the UK the Information Commissioners Office (ICO) has receive greater powers to audit and fine organizations that break privacy regulations. In addition, there are already laws due to be implemented that effect information sharing. In Europe these include 'Cookie Law' (Parliament, 2009) and in the UK the controversial Digital Economy Bill (Parliament, 2010), which imposes penalties for

[15] FIDIS (Future of Identity in the Information Society) is a NoE (Network of Excellence) supported by the European Union under the 6th Framework Programme for Research and Technological Development within the Information Society Technologies (IST) priority in the Action Line: "Towards a global dependability and security framework" (Future of Identity in the Information Society, 2010).

peer-to-peer file sharing of copyrighted material. This regulation will attempt to enforce privacy-related public policy for Internet cafes and Internet Users in the UK.

The EU's Article 29 Working Party released a report on the 26th of May 2010 revealing that the three major search engines, Yahoo, Google, and Microsoft, are not compliant with data protection law when managing information about online searches.

> "Personal data related to search queries is very sensitive, and search history should be treated as confidential personal data. This legal guidance (also found in FIP principles) indicates that the retention period shouldn't be longer than necessary for the specific purpose. Even if IP address or cookies are replaced by a unique identifier, the individual can still be identified by correlating stored queries." (Article 29 Data Protection Working Party, 2010)

The EU draft entitled "The Council Of Europe: The Consultative Committee Of The Convention For The Protection of Individuals with Regard To Automatic Processing of Personal Data" (Council of Europe, 2009) is intended to regulate information sharing transactions. This draft regulation explicitly deals with quality of consent and profiling, implements regulation, provides a much greater degree of notice to the individual, and therefore, (See section 5.1)

In the USA there are now state laws regarding information sharing. Massachusetts regulation 201 CMR 17.00 stipulates any business (in and out of Massachusetts) that holds personally identifiable information on residents of the state must encrypt that information during transit and storage. Proposed new federal legislation would require companies to get a user's explicit approval (that is, it would require users to "opt in") before those companies "knowingly collect" information about a person's medical history, financial records, Social Security number, sexual orientation or precise geographic location. (Ingram, 2010)

### Regulatory Calls for Participation

*FTC Roundtable (2009-2010)*

The US Federal Trade Commission in the US has hosted a series of day-long public roundtable discussions to explore the privacy challenges posed by the vast array of 21st century technology and business practices that collect and use consumer data. Such practices include social networking, cloud computing, online behavioral advertising, mobile marketing, the collection and use of information by retailers, data brokers, third-party applications, and other diverse businesses. The goal of the roundtables is to determine how best to protect consumer privacy while supporting beneficial uses of the information and technological innovation. More information is found at http://www.ftc.gov/bcp/workshops/privacyroundtables/

*National Strategy for Trusted Identities in Cyberspace*

The US Whitehouse and Department of Homeland Security (USDHS) have recently drafted a National Strategy for Trusted Identity in Cyberspace. The draft outlines an ambitious identity management strategy for the United States, but public discussion

has been extremely limited. The draft is a very significant and policy document which, if passed, will have an impact on Internet commerce, online speech, identity management, identity trust frameworks, and online anonymity. (USDHS, 2010)

*EU-US Consultation (2010)*

The European Commission invited "[a]ll stakeholders and organizations involved in the protection of personal data and/or processing, transfer or sharing of information for law enforcement purposes in the transatlantic context as well as the general public … to respond to the public consultation" on the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes. (European Commission, 2010b)

*European Commission: Public Consultation on Privacy (2009-2010)*

Article 8 of the Charter of Fundamental Rights of the European Union expressly recognizes the fundamental right to the protection of personal data. The Commission also engages in dialogue with non-EU/EEA countries to achieve a high level of protection of individuals when exporting personal data to those countries. It also initiates studies on the development at European and international level on the state of data protection and negotiates international agreements to safeguard the rights of individuals where their personal data are transferred (shared) to third countries for law enforcement purposes, such as the fight against terrorism and serious crime. (European Commission, 2010a)

*OECD Roundtables (2010a)*

Organisation for the Economic Co-operation and Development: 2010 was an important year for privacy, as the OECD marks the 30th anniversary of its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. (OECD, 1980) The Guidelines were the first international statement of the core information privacy principles and have proven highly influential over the years, serving as the basis for national and international privacy instruments. Several events took place in 2010, beginning on 10 March with an OECD Roundtable (OECD, 2010b) on the impact of the Privacy Guidelines.

*The UK Ministry of Justice*

The Ministry of Justice issued a call for evidence on the current data protection legislative framework, seeking views on:

1. How the European Data Protection Directive and the UK Data Protection Act are working
2. The impact of data protection on individuals and business, and
3. Whether the Information Commissioner's powers and penalties could be strengthened. (UK Ministry of Justice, 2010)

The responses will be assessed and used to inform the UK's position in negotiations on a new EU instrument for data protection, "which are expected to begin in early 2011." This fits in with the expected publication by end 2010 of the Commission's draft of the new EU data protection legislation. (Reding, 2010)

# Next Steps

Members of the Information Sharing Work Group continue to work towards a world where information sharing is a safe, trusted, and significant contributor to our lives.

## *Modeling Solutions*

Using the Customer-Supplier Engagement Framework, the ISWG is modeling long-term customer-supplier relationships, such as the Car Buying Engagement Model (Andrieu 2010b). These solutions must address the technical, business, and legal needs of all the participants in the system, from all individuals to all organizations.

## *Deploying Systems*

More than anything else, information sharing practices need interoperable real-world systems that sustainably deliver value to individuals. Working with VRM and user-centric identity advocates, the ISWG will continue to help individuals and companies bring information sharing products and services to market.

## *Standard Information Sharing Agreement*

In order to provide a legal foundation for individuals' control over shared information, the ISWG has started discussion and development of a Standard Legal Agreement that covers the use of shared information between parties. This agreement will allow individuals and information recipients to formally agree to the terms of use for common information sharing scenarios.

## *Information Sharing Trust Framework*

Mydex, a Community Investment Corporation in the United Kingdom, is leading the development of a Trust Framework to streamline automated recognition of organizations that agree to operate under the Standard Information Sharing Agreement.

## *Interoperability and Standards*

Information can only be shared effectively if the parties sharing it have a common understanding of the schema, the encoding, and mechanisms for transporting that information from party to party. The ISWG is working with the Internet Society, several working groups of the Kantara Initiative, ProjectVRM, and others, to develop, standardize, and test interoperable standards for information sharing.

## *Other Organizations*

Numerous organizations currently work in areas touching on information sharing. A partial list of such organizations can be found in Appendix A.

# Support

The Kantara Initiative and the Internet Society funded the original literature review.

This material is also based in part upon work supported by the National Science Foundation under Award Number IIP-0848990. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the National Science Foundation.

# References

Acquisti, A. (2004) *Privacy and Security of Information: Economic Incentives and Technical Solutions.* In J. Camp and R. Lewis (eds), *The Economics of Information Security*, Kluwer, 165-178.

Anderson, R., Heath, W., et al. (2009) *Database State.* Joseph Rowntree Reform Trust Ltd. [Online] http://www.jrrt.org.uk/uploads/Database%20State.pdf [Accessed ].

Andrieu, J. (2007a) *VRM: The user as point of integration.* June 14, 2007 [Online] http://blog.joeandrieu.com/2007/06/14/vrm-the-user-as-point-of-integration/ [Accessed July 24, 2010].

Andrieu, J. (2007b) *VRM and Personal Datastores.* July 26, 2007. [Online] http://blog.joeandrieu.com/2007/07/26/vrm-and-personal-datastores/ [Accessed August 14, 2010].

Andrieu, J. (2009) *Introducing User Driven Services.* April 26, 2009 [Online] http://blog.joeandrieu.com/2009/04/26/introducing-user-driven-services/ [Accessed June 7, 2010].

Andrieu, J. (2010a) *Beyond Data Ownership to Information Sharing.* January 21, 2010 [Online] http://blog.joeandrieu.com/2010/01/21/beyond-data-ownership-to-information-sharing/) [Accessed July 24, 2010].

Andrieu, J. (2010b) *Car Buying Engagement Model.* August 24, 2010 [Online] http://kantarainitiative.org/confluence/display/infosharing/Car+Buying+Engagement+Model) [Accessed August 24, 2010].

Article 29 Data Protection Working Party (2010a) *Signatories of the "Safer Networking Principles for the EU.* May 12, 2010, European Commission. [Online] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2010_05_12_letter_art29wp_signatories_safer_social_networking_principles_en.pdf [Accessed June 7, 2010].

Article 29 Data Protection Working Party (2010b) *Subject: Working Party 29 Data Protection Commissioners.* Letters from the Article 29 Working Party addressed to search engine operators (Google, Microsoft, Yahoo!). May 26, 2010 [Online] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf [Last Accessed June 7, 2010].

Australian Communications and Media Authority (ACMA) (2009), *Attitudes towards use of personal information online, Qualitative research report.* Aug. 2009. [Online] http://www.heinz.cmu.edu/~acquisti/papers/acquisti_eis_refs.pdf [Accessed 20 June 2010].

BBC (2010) *The Virtual Revolution, Episode Two: The Cost of Free.* [Online] Available in the U.K. at http://www.bbc.co.uk/programmes/b00qx4vy [Accessed 20 June 2010].

Bennett, L. (2009) *Reflections on privacy, identity and consent in on-line services.* Information Security Technical Report 143,, 119-123.

Broersma, M. (2010) *Breach Costs UK Companies £64 per record.* ZDNet 29 April, 2010 [Online] http://www.zdnet.co.uk/news/security-management/2010/04/29/breaches-cost-uk-companies-64-per-record-40088810/ [Accessed June 7, 2010].

Churchill, A. (2009) *Privacy and public policy delivery – Dichotomy or design.* Information Security Technical Report, Volume 14, Issue 3, August 2009, 131-137.

Cisco (2010) *Cisco Visual Networking Index: Forecast and Methodology, 2009-2014.* [Online] http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/whit

e_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html [Accessed July 1, 2010].

Cofta, P. (2007) *Trust, Complexity and Control - Confidence in a Convergent World.* John Wiley & Sons.

Council of Europe (2009) *DRAFT RECOMMENDATION ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA IN THE FRAMEWORK OF PROFILING.* October 2009, Secretariat document prepared by the Directorate General of Human Rights and Legal Affairs, European Commission. [Online] http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/T-PD-BUR_2009_02rev4_en.pdf [Accessed: June 7, 2010].

Elahi, S. (2009) *Privacy and Consent in the Digital Era.* Information Security Technical Report 14 (3), Aug. 2009:113-118.

European Commission (2010a) *Overview.* [Online] http://ec.europa.eu/justice_home/fsj/privacy/overview/index_en.htm [Accessed June 20, 2010].

European Commission (2010b) *Consultation on the future EU-US international agreement on personal data protection and information sharing for law enforcement purposes.* Consultation Questionnaire: http://ec.europa.eu/justice_home/news/consulting_public/0005/consultation_questionaire_en.pdf [Accessed August 22, 2010]; Answers to the Consultation Questionnaire: http://ec.europa.eu/justice_home/news/consulting_public/0005/registered_organisations/european_privacy_association_registered_en.pdf [Accessed August 22, 2010].

Facebook (2010) *Company Statistics.* [Online] http://www.facebook.com/press/info.php?statistics [Accessed June 20, 2010].

Federal Trade Commission (2007) *Fair Information Practices.* June 25, 2007 [Online] http://www.ftc.gov/reports/privacy3/fairinfo.shtm [Accessed June 7, 2010].

Future of Identity in the Information Society (2010), *Home: The Future of Identity in the Information Society.* [Online] http://www.fidis.net [Accessed August 22, 2010].

Glazer, I. and Blakely, B. (2009) *Privacy.* Technology Thread: Policy, Privacy, and Personalization, Ver. 1.0, Apr 03, 2009, Burton Group.

Henderson, Iain (2009) *The Personal Data Eco-System.* [Online] http://kantarainitiative.org/wordpress/2009/06/iain-henderson-the-personal-data-eco-system/ [Accessed June 2, 2010].

IBM Global Services (2006) *The Toxic Terabyte.* [Online] http://www-935.ibm.com/services/us/cio/leverage/levinfo_wp_gts_thetoxic.pdf. [Accessed November 11, 2009].

Ingram, M. (2010) *Congress Proposes Sweeping Internet Privacy Bill.* [Online] http://business-news.thestreet.com/technology-news/2010/05/04/a/622924345-congress-proposes-sweeping-internet-privacy/ [Accessed June 7, 2010].

ISWG (2009) *Go To Market Space.* July 31, 2009 [Online] http://kantarainitiative.org/confluence/download/attachments/11239426/go+to+market+space.tiff [Accessed July 29, 2010].

Jaquet-Chiffelle, David-Olivier & Buitelaar, Hans. (2009) D17.4: *Trust and Identification in the Light of Virtual Persons.* WP17: The FIDIS (Future of Identity in the Information Society) Consortium 2009,. [Online] http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp17-

del17.4_Trust_and_Identification_in_the_Light_of_Virtual_Persons.pdf [Accessed 20 June 2010].

Kelly, Kevin (2008) *Better than Free* [Online] http://www.kk.org/thetechnium/archives/2008/01/better_than_fre.php [Accessed August 14, 2010].

Kirby, Michael, The Honourable (2010) *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy.* Organisation for the Economic Co-operation and Development. [Online] http://www.oecd.org/dataoecd/4/62/44945835.doc [Accessed August 22, 2010].

Kuner, Christopher (2009) 'Internet Jurisdiction and Data Protection Law: An International Legal Analysis.' (August 30, 2009) *International Journal of Law and Information Technology, 2010.* [Online] http://ssrn.com/abstract=1496847 [Accessed August 22, 2010].

Lacohée, H., Crane, S., and Phippen, A., (2006) *Trustguide: Final Report, October 2006.* [Online] http://trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf [Accessed 20 June 2010].

Lauchlin, S. (2009) *CRM market growing but set for tougher times.* MyCustomer.com [Online] http://www.mycustomer.com/topic/technology/crm-market-growing-set-tougher-times-2009 [Accessed August 22, 2010].

Lee, E. (2010) *Draft of Online Privacy Bill Stirs Fears Among Ad Industry.* Advertising Age, May 4, 2010. [Online] http://adage.com/digital/article?article_id=143690 [Accessed June 7, 2010].

Levine, R., Locke, C., Searls, D., and Weinberger, D. (1999) The Cluetrain Manifesto: The End of Business as Usual. [Online] http://cluetrain.com/ [Accessed August 24, 2010]

Lewis, N., (2009) *Rethinking privacy and trust.* Battle of Ideas, October 20, [Online] http://www.battleofideas.org.uk/index.php/2009/battles/3457/ [Accessed June 7, 2010].

Liedtke, M., (2010) *Google's Profit Up 37 Percent In 1Q As Revenue Hits $5 Billion.* Huffington Post, Apr. 15, 2010. [Online] http://www.huffingtonpost.com/2010/04/15/google-profit-up-37-perce_n_539609.html [Accessed August 22, 2010].

Maier, F., (2009) *How Building Trust Can Boost Online Sales*. ComputerWorld http://www.computerworld.com/s/article/9137197/How_Building_Trust_Can_Boost_Online_Sales?taxonomyId=0&pageNumber=1 [Last Accessed July 7, 2010].

Maler, Eve (2010a) *UMA Explained.* July 15, 2010 [Online] http://kantarainitiative.org/confluence/display/uma/UMA+Explained [Accessed August 14, 2010].

Maler, Eve (2010b) *WG - User Managed Access Home.* August 10, 2010 [Online] http://kantarainitiative.org/confluence/display/uma/Home [Accessed August 14, 2010].

McNish, J., and El Akkad, O., (2010) *Facebook users risk blackmail, privacy czar warns.* The Globe and Mail, Technology, April 23, 2010. [Online] Available at: http://www.theglobeandmail.com/news/technology/facebook-users-risk-blackmail-privacy-czar-warns/article1545444/ [Accessed 20 June 2010].

MiniWatts Marketing (2010) *Internet Usage Statistics: The Internet Big Picture: World Internet Users and Population Stats*. [Online] http://www.internetworldstats.com/stats.htm [Accessed 14th June 2010].

Mitchell, A., Brandt, L., et al. (2009) *The New Personal Communication Model: The Rise of Volunteered Personal Information.* Ctrl-Shift [Online] http://ctrl-shift.co.uk/vpi-report/

Moblen, Even (2010) Written testimony to US House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade & Consumer Protection. December 2, 2010. Online http://online.wsj.com/public/resources/documents/Moglen.Testimony.12.02.2010.pdf Accessed December 4, 2010.

Morrone, A., Tontoranelli, N., and Ranuzzi, G., (2009) *How Good Is Trust? Measuring Trust And Its Role For The Progress Of Societies*. Organisation for Economic Co-operation and Development: 38.

Mydex, (2010) *Individual-centric Research* April 2010 [Unpublished]

Nielson, (2010) *U.K. Web Use Up 65% Since 2007 – Social Networking more than Doubles.* NielsonWire. May 20, 2010. [Online] http://blog.nielsen.com/nielsenwire/global/u-k-web-use-up-65-since-2007-social-networking-more-than-doubles/ [Accessed August 14, 2010]

Nissenbaum, Helen (2004) *Privacy as Contextual Integrity.* Washington Law Review: Vol. 79, No. 1, pp. 101-139. [Online] http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID553661_code139145.pdf?abstractid=534622&mirid=1 [Accessed 20 June 2010].

Number 10, (2010) *Queen's Speech – Freedom* (Great Repeal) Bill, May 25, 2010 The official site of the Prime Minister's Office [Online] http://www.number10.gov.uk/queens-speech/2010/05/queens-speech-freedom-great-repeal-bill-50647 [Accessed June 7, 2010]

OECD (2010a) *The 30th Anniversary of the OECD Privacy Guidelines.* Organisation for the Economic Co-operation and Development. [Online] http://www.oecd.org/document/35/0,3343,en_2649_34255_44488739_1_1_1_1,00.html [Accessed August 22, 2010].

OECD (1980) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Background.* Organisation for the Economic Co-operation and Development. [Online]

OECD (2010b) *30 Years After: the Impact of the OECD Privacy Guidelines.* Organisation for the Economic Co-operation and Development, event held on March 10, 2010 in Paris France. [Online] http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html [Accessed August 22, 2010].

Ohm, P. (2009) *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*. University of Colorado Law Legal Studies Research Paper No. 09-12.

OIX (2010) *The U.S. Government ICAM Trust Framework.* [Online] http://openidentityexchange.org/trust-frameworks/us-government-icam [Accessed July 7, 2010].

PARLIAMENT, T. E. (2009) *DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, amending Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector. Directive 2002/58/EC. D. O. T. E. P. A. O. T. C. O. Europe. [Online] http://register.consilium.europa.eu/pdf/en/09/st03/st03674.en09.pdf [Accessed June 7, 2010].

PARLIAMENT, T.E. (2010) *Digital Economy Act 2010*. United Kingdom [online] http://www.opsi.gov.uk/acts/acts2010/ukpga_20100024_en_1 [Accessed June 7, 2010]

ProjectVRM (2010) *About*. [Online] http://blogs.law.harvard.edu/vrm/about/ [Accessed August 22 2010].

ProjectVRM Wiki (2009) *Personal RFP.* [Online] http://cyber.law.harvard.edu/projectvrm/Personal_RFP [Accessed August 14, 2010].

Reding, Viviane (2010) *Next Steps for Justice, Fundamental Rights and Citizenship in the EU.* Speech/10/108, March 18, 2010. [Online] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/108&format=HTML&aged=0&language=EN&guiLanguage=en [Accessed August 22, 2010].

Rundle, M. (ed.) (2010) *The Open Identity Trust Framework (OITF) Model* March 2010 [Online] http://openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf [Accessed August 25, 2010]

Searls, D., (2009) *Get ready for fourth party Services Linux Journal.* [Online] http://www.linuxjournal.com/content/get-ready-fourth-party-services [Accessed July 29, 2010]

Seligman, A., (1997) *The Problem of Trust.* Princeton (University Press, Princeton New Jersey).

Solove, D. (2004) *The Digital Person: Technology and Privacy in the Information Age*. GWU Law School Public Law Research Paper No. 121, New York University Press.

The Gallup Organization (2008) *Data Protection in the European Union; Citizens' Perceptions.* Flash Eurobarometer Series #225:137.

TRUSTe, (2006) *Survey: A false sense of online security.* [Online] http://www.truste.org/about/press_release/12_06_06.php [Accessed: November 11, 2009]

UK Ministry of Justice (2010) *Call for Evidence on the data protection legislative framework.* [Online] http://www.justice.gov.uk/consultations/call-for-evidence-060710.htm [Accessed August 22, 2010].

UK Ministry of Justice (2010b) Tech and Law: Data Protection Directive - reform proposals due by end 2010. [Online] http://blog.tech-and-law.com/2010/03/data-protection-directive-reform.html [Accessed August 22, 2010].

USDHS (2010) *National Strategy for Trusted Identities in Cyberspace.* Draft strategy document. [Online] http://www.dhs.gov/xlibrary/assets/ns_tic.pdf [Accessed August 22 2010].

Watson, R., Piccoli, G., et al. (2003) *Customer-Managed Interactions: A New Paradigm for Firm-Customer Relationships.* [Online, PowerPoint presentation] http://misqe.org/ojs2/index.php/misqe/article/view/80 [Accessed June 15, 2010].

Whitley, A. E., (2009) *Informational Privacy, Consent and the 'Control' of Personal Data*. EnCoRe Publication London School of Economics: 15.

Whitehead, T. (2009) *Data losses and breaches up by half.* The Telegraph, 11 Nov 2009 [Online] http://www.telegraph.co.uk/news/uknews/law-and-order/6539206/Data-losses-and-breaches-up-by-half.html [Accessed July 7, 2010].

Wikimedia (2010) *Wikipedia Page Views: Sunday June 13, 2010.* [Online] http://stats.wikimedia.org/EN/TablesPageViewsMonthly.htm [Accessed 13th June 2010].

YouTube (2010) *YouTube Fact Sheet.* [Online] http://www.youtube.com/t/fact_sheet [Accessed 14 June 2010].

Zekos, Georgios (2007) 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction.' *International Journal of Law and Information Technology Vol. 15 No. 1* Oxford University Press.

# Appendix A: IS Organizations and Initiatives

List of Information Sharing Organizations/Research Efforts

### Article 29 Working Party

http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm
Article 29 WP is a data protection group working under the EU commission Justice and Home Affairs.

### DataPortability Project

http://www.dataportability.org/
Project working on policies and practices for allowing personal data to be portable.

### EID - STORK

https://www.eid-stork.eu/
STORK is a competitiveness and innovation framework program, co-funded by EU. It aims at implementing an EU wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State.

### EnCoRe (*Ensuring Consent and Revocation*)

http://www.encore-project.info/
Ensuring Consent and Revocation is a research project, being undertaken by UK industry and academia, to give individuals more control over their personal information.

### EUROPRISE

https://www.european-privacy-seal.eu/
The European Privacy Seal for IT Products and IT-Based Services

### FIDIS (*Future of Identity in the Information Society*)

http://www.fidis.net/
FIDIS is a “Network of Excellence” supported by the European Union under the 6th Framework Programme for Research and Technological Development. Their working “towards a global dependability and security framework.”

### ISOC (*Internet Society*)

http://www.isoc.org/
The Internet Society is an independent international nonprofit organization founded in 1992 to provide leadership in Internet related standards, education, and policy around the world.

### ISTPA (*International Security Trust and Privacy Alliance*)

http://www.istpa.org/

**OECD**

http://www.oecd.org/document/35/0,3343,en_2649_34255_44488739_1_1_1_1,00.html
The OECD is currently working on the updating the Privacy guidelines from 1980.

**OITF (*Open Identity Trust Framework*)**

http://www.openidentityexchange.org
Open Identity Trust Framework recently released a document on identity trust framework for the USA governments open identity initiative.

**PrimeLife**

http://www.primelife.eu/
“Bringing sustainable privacy and identity management to future networks and services.” This is a research project funded by the European Commission’s 7th Framework Programme.

**Project VRM**

http://projectvrm.org/
ProjectVRM is a research and development project of the Berkman Center for Internet & Society at Harvard University focused on Vendor Relationship Management.

**TAS**

http://www.tas3.eu/
TAS³ is building an “end2end trust architecture for services related to personal information.” The goal is to 'automate' the data sharing all while providing user-controlled access to such data. This involves regional-sectoral-national trust networks on specific domains such as employability en e-health.

**VOME**

http://www.vome.org.uk/
Researchers from the Information Security Group (ISG) at Royal Holloway, University of London, Salford and Cranfield Universities are participating in a three year collaborative research project with consent and privacy specialists at Consult Hyperion and Sunderland City Council, to explore how people engage with concepts of information privacy and consent in on-line interactions.

**WC3 (*World Wide Web Consortium*)**

http://www.w3.org/
The World Wide Web Consortium (W3C) is an international community that develops standards to ensure the long-term growth of the Web.

# Revision History

| Version | Date | Modified by | Comment |
|---|---|---|---|
| Work Group Report.v3 | December 6, 2010 | Joe Andrieu | Edits for clarity, added Moglen quote |
| Work Group Report.v2 | November 22, 2010 | Judi Clark | Revised and edited text to flow more logically |
| Work Group Report | October 25, 2010 | Judi Clark | Work group report format |
| draft report | October 23, 2010 | Joe Andrieu | Prepared for work group approval |
| draft for review.v3 | October 3, 2010 | Judi Clark | formatted per Kantara template |
| draft for review.v2 | August 25, 2010 | | |
| draft for review.v1 | August 17, 2010 | | |
| working draft.v5 | August 13, 2010 | | |
| working draft.v4 | August 4, 2010 | | |
| working draft.v3 | July 19, 2010 | | |
| working draft.v2 | June 22, 2010 | Judi Clark, Iain Henderson, Mark Lizar | Second draft. |
| working draft.v1 | June 20, 2010 | Mark Lizar | First draft. |