



The Personal Network: A New Trust Model and Business Model for Personal Data

Drummond Reed & Joe Johnston, Connect.Me; Scott David, K&L Gates

Executive Summary

The explosive growth of social networks has created an entire social layer for the Internet, changing its very role in society. This white paper explores the emergence of the next layer: the *personal network*. It explains the legal and economic reasons personal networks differ from social networks and introduces the Respect Trust Framework, the first trust framework designed expressly for personal data. It steps through how the core components of personal networking—trust anchors, contexts, and person-to-person contextual vouching—are woven together to create a strong, resilient trust fabric. Finally it covers the business model for personal networks and why it differs markedly from the advertising-driven model of social networks.

INTRODUCTION	2
PART ONE: THE TRUST MATRIX	4
PART TWO: THE RESPECT TRUST FRAMEWORK™	8
PART THREE: THE TRUST MODEL	11
PERSONAL DATA LOCKERS AND PERSONAL CLOUDS	11
CONNECTIONS	12
CONTEXTS	13
VOUCHING	14
TRUST ANCHORS	15
FOUNDING TRUST ANCHORS	17
PART FOUR: THE BUSINESS MODEL	19
FUTURE WORK	22
OPEN IDENTITY EXCHANGE (OIX)	22
PERSONAL DATA ECOSYSTEM CONSORTIUM (PDEC)	22
WORLD ECONOMIC FORUM (WEF) RETHINKING PERSONAL DATA PROJECT	22
MYDEX COMMUNITY INTEREST CORPORATION (CIC)	22

Introduction

The spectacular success of social networking services like Facebook, Twitter, LinkedIn, and others has done more than just change the face of the net—it has changed the face of the world. For example, while historians will debate for years exactly how much the social messaging capabilities of Facebook and Twitter contributed to the 2011 “Arab Spring”, no one denies it was a critical factor.

The sheer size of Facebook (600 million users), Twitter (200 million), and LinkedIn (100 million) as online social communities is also unprecedented.¹ Put simply, the Internet’s ability to connect people to each other has become the defining characteristic of online activity in the last half decade. In the past year, Mark Zuckerberg was named TIME Magazine’s Person of the Year, and the movie *The Social Network* was in close contention for the Oscar for Best Picture.

This growth has been accompanied by a steady drumbeat of concerns about the impact on personal privacy. A scant three months after TIME’s Person of the Year article, TIME carried a different cover story called [Your Data: For Sale](#).²

It has been wryly observed that, with regards to amassing personal data, “Facebook has achieved in six years what world governments have not been able to achieve in six centuries.” This is not to say that Facebook, or any other social network, is doing anything wrong. As it is often pointed out, users of Facebook and other social networks provide their data voluntarily, and with the expectation that much of it will be publicly available.



However the success of these social networks does not dictate that their technical, legal, and economic models for personal data apply everywhere. Take, for example, electronic health records (EHR). Although it has become a major economic and legislative imperative (at least in the U.S.) to migrate to EHR to cut costs and improve care, the central tenets of EHR networks such as the [U.S. National Health Information Network](#) (NHIN)³ stand in marked contrast to those of centralized social networks:

- Patients have exclusive control over their EHR; sharing only happens with their explicit permission.
- There is no centralized repository—every patient and health care provider work with their choice of EHR service provider in an interoperable system.
- EHR data is portable among EHR service providers, and patients may switch between providers just like they may switch banks or wireless providers.

¹ <http://en.wikipedia.org/wiki/Facebook>, <http://en.wikipedia.org/wiki/Twitter>, <http://en.wikipedia.org/wiki/LinkedIn>

² <http://www.time.com/time/covers/0,16641,20110321,00.html>

³ <http://en.wikipedia.org/wiki/NHIN>

While these requirements for electronic health records may appear specialized, in fact they may be gainfully applied to almost any form of data where privacy and personal control are desired. This suggests another step in the evolution of information sharing networks—a step that builds on top of the social layer the same way the social layer built on the Web.

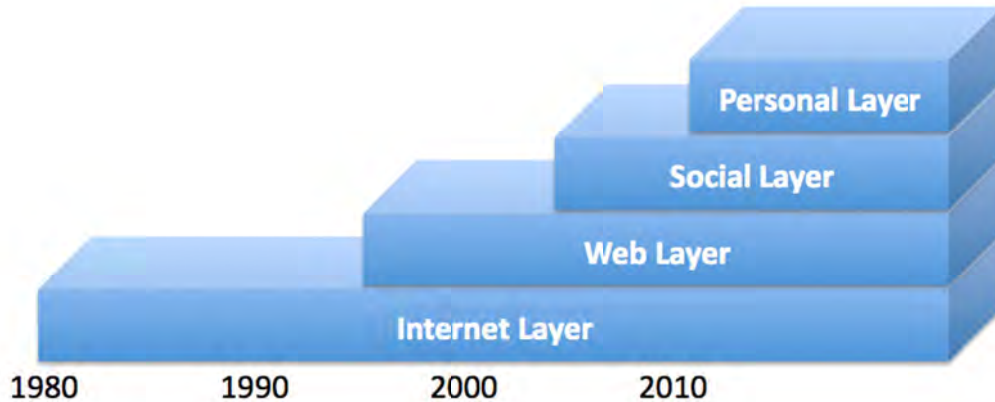


Figure 1: The personal layer will build on the social layer

This new layer is *personal*; it will be implemented through *personal networks*. This paper introduces the key concepts of personal networking in four sections:

1. **Part One: The Trust Matrix** provides an analysis of why personal networks require a different legal and economic architecture than social networks.
2. **Part Two: The Respect Trust Framework™** introduces a legal solution to providing the level of control necessary for a personal network to be trusted.
3. **Part Three: The Trust Model** shows how the Respect Trust Framework can be implemented via a contextual trust network rooted in individuals.
4. **Part Four: The Business Model** explains the economic model for how a personal network can thrive by protecting, rather than exploiting, the personal data of its members.

Part One: The Trust Matrix

The market for CRM (Customer Relationship Management) software and services has grown to over \$14B annually in the last decade. This represents the current value to businesses of being able to aggregate information about their customers into one consolidated view to help maximize each customer's lifetime value.⁴

In the context of business-to-consumer relationships, this also creates a large information imbalance. Businesses have the tools, IT staff, and resources to perform this aggregation; consumers do not. So although purpose of this aggregation is to serve the customer, it still creates the fundamental tension illustrated in Figure 2.

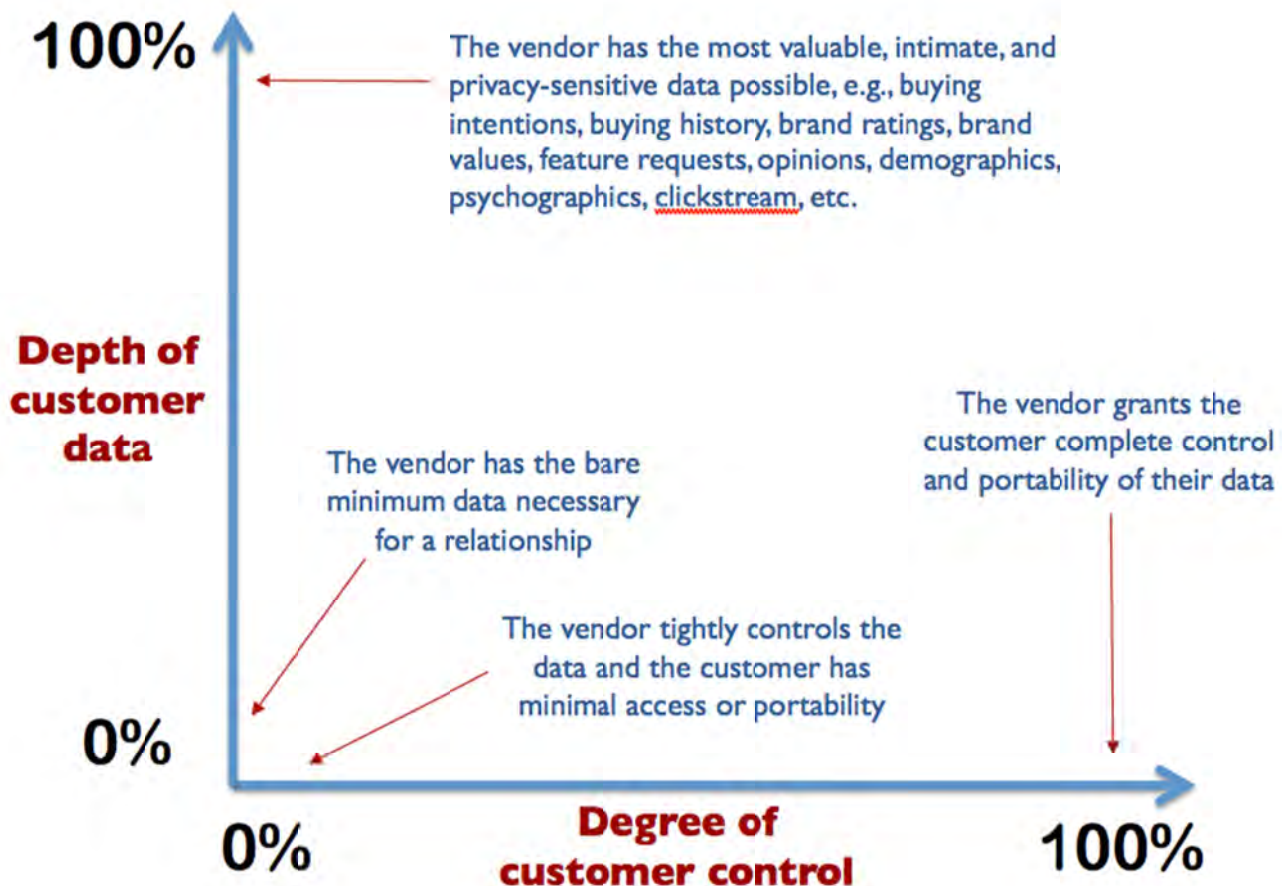


Figure 2: The Trust Matrix

This **trust matrix** represents the tradeoff between the amount of information a customer is willing to share with a business and the degree of control the business is willing to grant the customer over this information. A classic example is an email address: most customers will only share it with a business if they trust the business not to send them spam or sell it to third parties without the customer's consent.

⁴ http://en.wikipedia.org/wiki/Customer_lifetime_value

All major categories of relationship management can be plotted on this matrix.

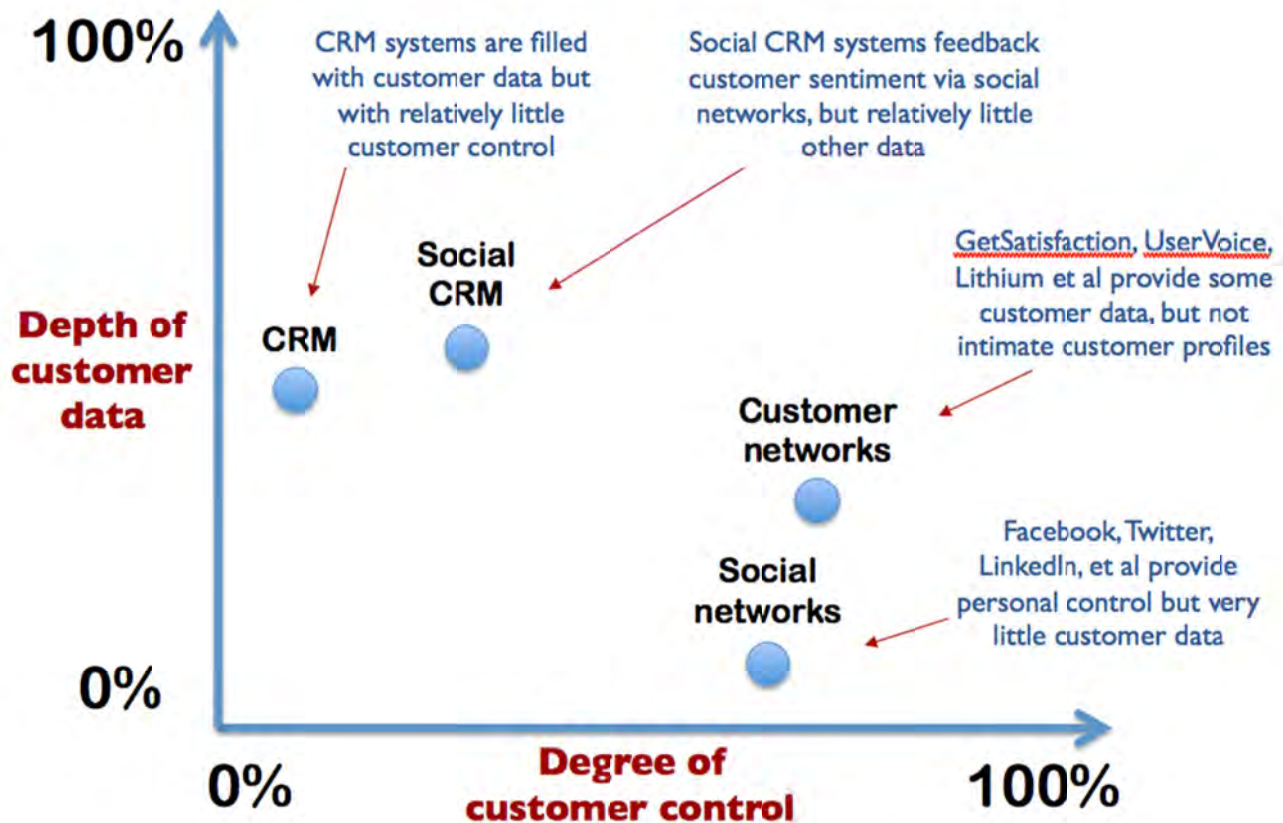


Figure 3: Plotting existing solutions on the Trust Matrix.

CRM systems aggregate as much customer data as can benefit a business, but most are designed to give the business near-exclusive control over that data. To the extent customers have access, it is usually for self-service and as required to fulfill privacy, regulatory, and Fair Information Practices compliance requirements.

Social CRM, a very active trend in the CRM space, involves adding social media feedback features to traditional CRM systems so they can be more directly attuned to customer discussions on the social web. With social CRM, businesses can “listen” to social networks and gain some incremental knowledge about customer sentiments, but only a modest amount of new customer data.

Social networks are at the other side of the matrix: they give individuals much more control over the data they share and the friends they share it with, but since they are serving social relationships, they produce relatively little customer data.

Customer networks such as GetSatisfaction™, UserVoice™, and Lithium™ harness the power of social networking within a community of customers. Because they are directed at customer needs in the context of specific businesses, they can produce significantly more relevant data, while at the same time giving customers the freedom of expression and engagement they enjoy on social networks.

Note how the plotting of these existing solutions reveals a trough down the diagonal access of the matrix. This suggests the presence of two key thresholds:

1. The first is the threshold of a customer's trust if a **business** holds and controls all their data. Conventional and social CRM systems both fall within this threshold, because the database of the customer's information is managed almost exclusively by the business.
2. The second is the threshold of trust if the data is held by a **third party**, such as a social network or customer network. This threshold is higher because the customer has greater control, and to a certain extent trusts the third party not to share the data indiscriminately with businesses. However most third parties are paid by businesses, through advertising or other services, so to a certain extent their interests must be aligned.

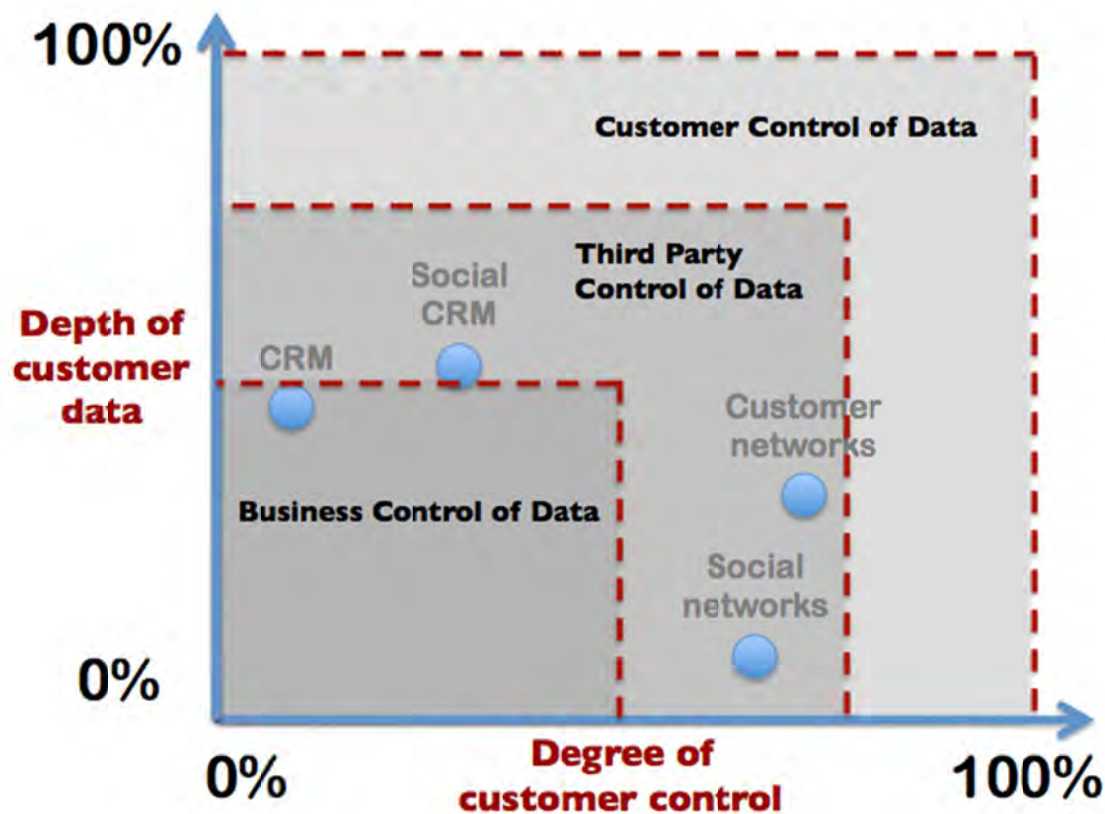


Figure 4: The thresholds of business and third party control of data

To step beyond this third-party threshold requires giving customers direct control of their personal data in the same way they control their money in their bank account. A customer may take on this role directly, or use a service provider to assist them. In legal terms, such a provider is called an **agent**. Where an agent has control of money or financial assets, it is called a **fiduciary**, and it is the highest standard of care under the law.⁵ Another example is

⁵ <http://en.wikipedia.org/wiki/Fiduciary>

real estate, where a **buyer's agent** has the duty is to represent the interests of a buyer, not the seller, in a transaction.⁶

What this suggests is the need for a new type of agent: a service provider whose duty is to *represent the interests of individuals in the exchange of personal data*. Such a **personal data agent** would give people the control they need to be confident sharing the deepest, richest customer data—the data about their activities, intentions, and aspirations that they will only willing to share if they have much more control of when, where, and how this information is used.⁷ A network of people and persona data agents could be characterized as either “a personal CRM system” or “a people’s network”. Put these two together and you have the **personal network**.

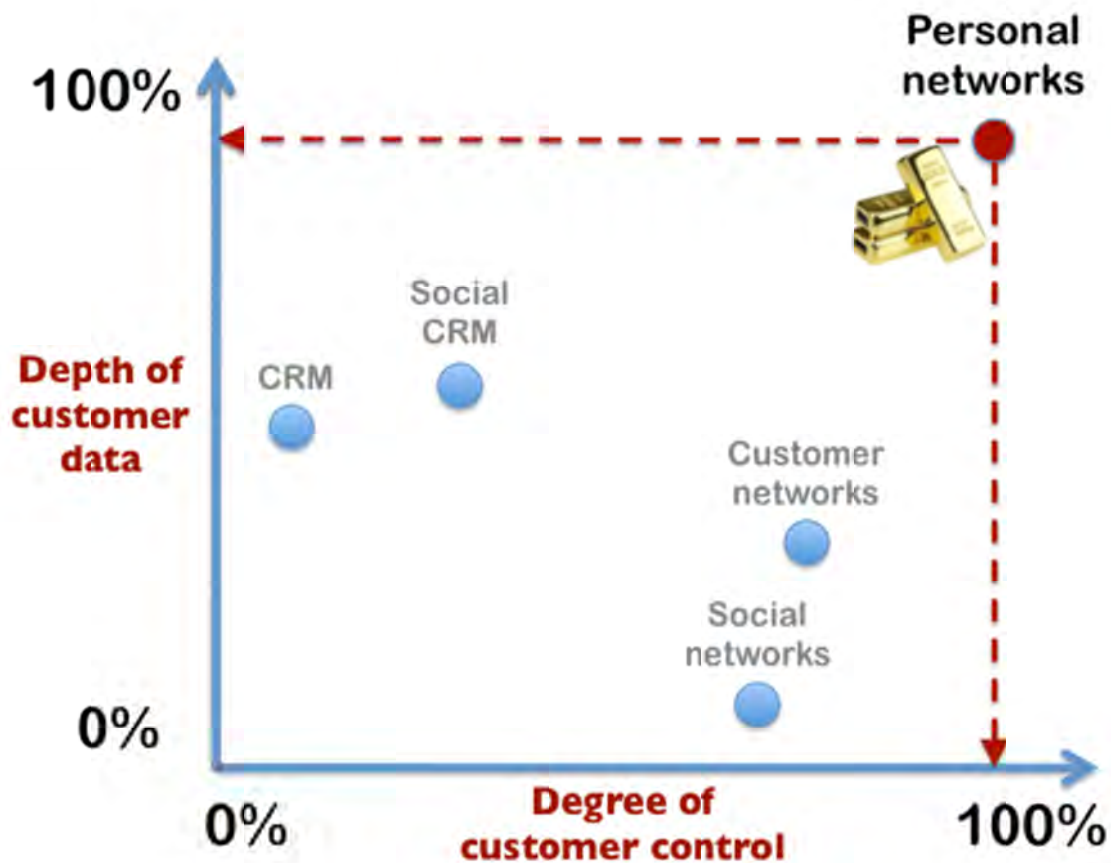


Figure 5: A personal network provides the level of control needed to unlock the sharing of rich customer data with businesses

By providing the very high degree of measurable control and protection needed for the trusted sharing of personal data, a personal network can serve as a platform for personal networking applications and services that will be as empowering in the next decade as social networking was in the last decade.⁸

⁶ http://en.wikipedia.org/wiki/Buyer's_agent

⁷ In Vendor Relationship Management (VRM - <http://projectvrm.org>), this is called a “fourth party”. See Doc Searls, <http://blogs.law.harvard.edu/vrm/2009/04/12/vrm-and-the-four-party-system/>.

⁸ See Julian Gay, *The Rise of the Social Customer*, <http://www.sdforum.org/SDForum/Assets/PDFs/Newsletters/sdforum-newsletter-fall-2010.pdf>

Part Two: The Respect Trust Framework™

In both social networks and personal networks, members enter into a contractual relationship with the network provider. For social networks, this is typically a terms of service (TOS) agreement over which the network provider has exclusive control. For a personal network, this contract must differ in at least three key respects:

1. First, it must create the **personal data agent relationship**, i.e., it must specify that the member controls the personal and/or private data the member shares via the network, and that the network provider has a duty not just to protect this data, but to respect the member's right to control it.
2. Secondly, to be consistent with #1, the contract must not give the network provider the unilateral right to change the contract, but must **involve members in a process for approving modifications**.
3. Thirdly, in a multi-provider network, the contract must **cover all service providers in the network**, and must enable members to switch between personal data agents the same way customers can switch between banks or wireless service providers and retain their money and phone numbers.

This last point is particularly important because virtually **all large-scale trust networks are multi-provider markets**. Examples include the international banking, credit card, ATM, telephone, and domain name systems. Each of these markets depends on the establishment of standard contract terms to assure that all participants act in reliable and predictable ways. This is why the Internet identity industry developed the **trust framework**, a mechanism that enables all the parties to a federated identity system to be bound by (and receive the benefits of) a common set of legal and technical rules. Figure 6 illustrates the “trust triangle” of relationships that operate under the umbrella of a trust framework.

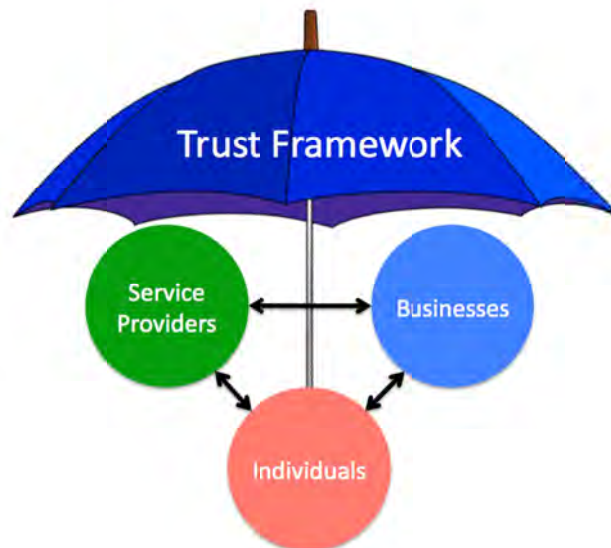


Figure 6: The “trust triangle” of relationships covered by online trust frameworks

[Open Identity Exchange](http://openidentityexchange.org)⁹ was launched in March 2009 to serve as the first international non-profit organization providing listing and administrative services for trust frameworks developed under [The Open Identity Trust Framework Model](http://www.openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf).¹⁰ The first OIX listed trust framework was the [U.S. ICAM Trust Framework](http://openidentityexchange.org/trust-frameworks/us-icam),¹¹ developed to meet the needs of the United States government as a relying party for federated login services such as OpenID. Other OIX trust frameworks are in development for telecom and public media.¹²

These OIX trust frameworks are being developed from the standpoint of the businesses, government agencies, or industries that need them. In March 2011 Connect.Me™ joined OIX to list the first open identity trust framework developed from the standpoint of *individuals*—one designed for the sharing of personal data protected under the personal data agent model across all international jurisdictions. It is called the **Respect Trust Framework**¹³ after the five core principles upon which it is based.¹⁴

Principle	Synopsis	Wording
Promise	<i>We will respect each other's digital boundaries</i>	Every member promises to respect the right of every other member to control the identity and personal data they share within the network and the communications they receive within the network.
Permission	<i>We won't steal from each other or try to fool each other online</i>	As part of this promise, every member agrees that all sharing of identity and personal data and sending of communications will be by permission, and to be honest and direct about the purpose(s) for which permission is sought.
Protection	<i>We will keep the confidences entrusted in us</i>	As part of this promise, every member agrees to provide reasonable protection for the privacy and security of identity and personal data shared with that member.
Portability	<i>We won't hold each other hostage</i>	As part of this promise, every member agrees to ensure the portability of the identity and personal data shared with that member.
Proof	<i>We will reasonably cooperate for the good of all members</i>	As part of this promise, every member agrees to share the reputation metadata necessary for the health of the network, including feedback about compliance with this trust framework, and to not engage in any practices intended to game or subvert the reputation system.

Table 1: The five core principles in the Respect Trust Framework

⁹ <http://openidentityexchange.org>

¹⁰ <http://www.openidentityexchange.org/sites/default/files/the-open-identity-trust-framework-model-2010-03.pdf>

¹¹ <http://openidentityexchange.org/trust-frameworks/us-icam>

¹² <http://openidentityexchange.org/working-groups>

¹³ <http://openidentityexchange.org/trust-frameworks/respect-trust-framework>

¹⁴ Also named after the seventh principle of Privacy By Design: *Respect for Users*. See <http://www.privacybydesign.ca/about/principles/>

Scott David, principal legal architect of the Respect Trust Framework, summarizes these principles as **the golden rule for data**: *treat data about others as you would like them to treat data about you*.¹⁵ This is consistent with its purpose: to serve as the contract binding all members of a personal network in which members agree to undertake the **personal data agent obligation** to represent the interests of the individual in the sharing and usage of their personal data.

It is important to emphasize that it goes beyond just protecting privacy. In fact the first three principles alone comprise an operational definition of privacy:

Privacy is a **promise of permission and protection**.

The other two principles, **portability** and **proof**, speak to other equally important elements of reciprocity in human relationships:

- **Portability** is the ability to move data about you from one product, site, business, or service provider to another without unreasonable constraint. This adds significantly to the value of the data for the sum of all parties concerned—“the network effect for data”.¹⁶ For specific examples, see the [Portability Policy](#) work of the [DataPortability Project](#).¹⁷
- **Proof** is the ability to have ones identity and reputation accurately reflected by others. See the next section for a full discussion.

A trust framework that encompasses all five of these key principles can unlock a new class of personal networking applications that deliver at least as much new value as we have received from social networking applications. This is the new category of value that reflects the positive upside of privacy: **respect**.



Figure 7: Respect is the upside of privacy

¹⁵ http://en.wikipedia.org/wiki/Golden_rule

¹⁶ http://en.wikipedia.org/wiki/Network_effect

¹⁷ <http://portabilitypolicy.org/> and <http://dataportability.org/>

Part Three: The Trust Model

Personal Data Lockers and Personal Clouds

The starting premise of a personal network is that every individual member controls their own store of personal data, commonly referred to as a **personal data locker**.¹⁸ This store can be in one place or it can be virtual, i.e., distributed across any number of devices and locations, although it is most useful if at least part of it is accessible on a server “in the cloud”. For this reason the set of personal devices (smartphones, laptop computers, GPS, etc.) that can access, manage, and share personal data via a personal data locker is called a **personal cloud**.



Figure 8: A personal cloud is the set of devices that share a personal data locker

The promise of control in the Respect Trust Framework begins with an individual’s choice of hosting for their personal data locker. There are two basic options:

1. **Self-hosting** is just like hosting your own blog, email, or Web server. You as an individual have direct control over your locker.
2. **Cloud hosting** is analogous to outsourcing the operation of blog, email, or Web server to a third-party hosting company. The key difference is that under the Respect Trust Framework this service provider is **obligated to act in the legal role of a personal data agent**.

As personal networking grows, many different types of companies may become personal cloud providers, including telcos, banks, news organizations, email and Web hosting providers, cloud service providers, and online data backup companies.

¹⁸ See David Siegel, <http://thepowerofpull.com/pull/foundations/personal-data-locker>

Connections

Just as a social network makes it much easier to share information with friends, a personal network makes it much easier and safer to for an individual to share personal data over at least three types of connections:

1. **Person-to-person** connections are with other individuals on the network. In most cases this will be a superset of one's social networking friends, but a key difference is that a personal network will let you connect with a friend *anywhere, on any social network*. Personal network connections are never constrained by who is on what social network.
2. **Person-to-community** connections are with any group of people who share a common personal interest. A typical example is a household—it joins the group of people who live together in it. Clubs, sports, hobbies, books—any other mutual interest can form a community.
3. **Person-to-business** connections are with businesses or organizations who join the network in order to have direct personal relationships under the terms of the Respect Trust Framework. Person-to-business connections play a special role in the economics of a personal network—see the next section.

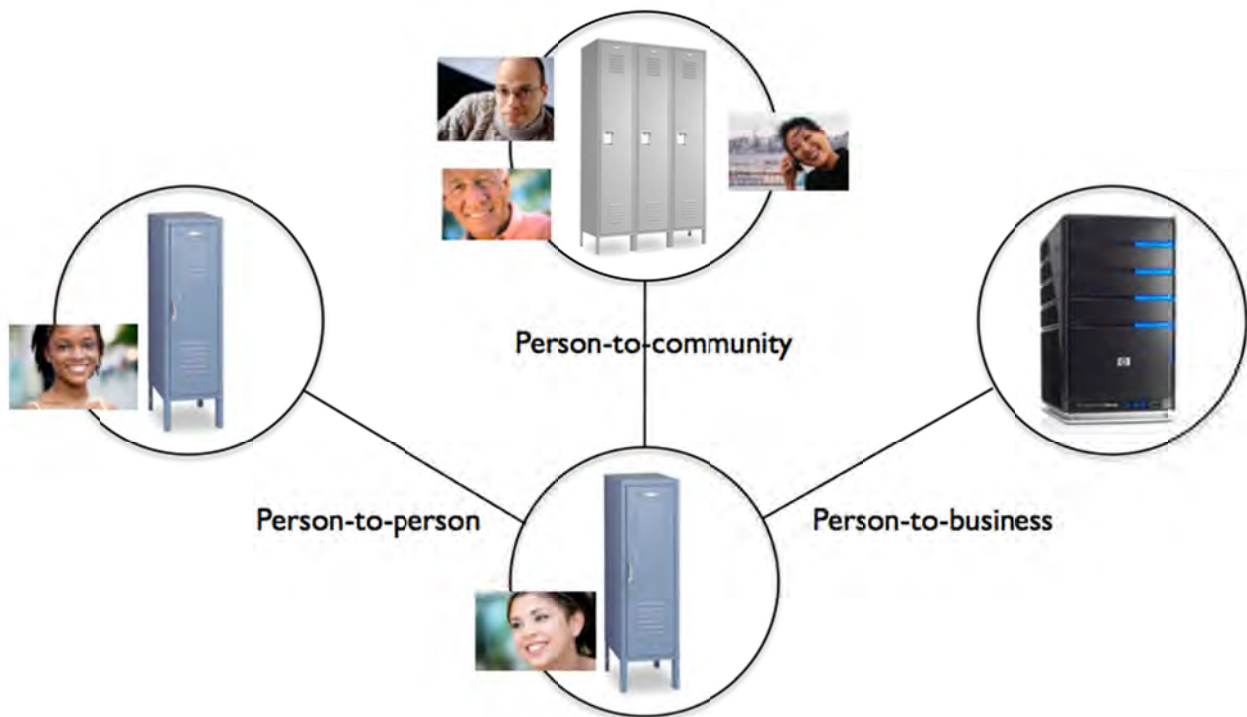


Figure 9: The three types of connections on a personal network

Contexts

The heart of a social network is the **social graph**: the map of who knows whom. A social graph becomes much more valuable when overlaid with a **context graph**, i.e., the map of which relationships belong in which contexts.

For example, a college student may know people in all of these contexts: family, relatives, childhood friends, neighbors, high school classmates, college roommates, sports teammates, and professors. Understanding which relationships fall into which contexts can make it much easier to share context-specific information.

It can also solve awkward social situations such as the [teacher friending problem](#) discussed by Microsoft social software researcher Danah Boyd: what should a teacher do when a student asks to friend them on Facebook? ¹⁹ Allow a link to the same page where the teacher shares photos and stories with old college friends?

Figure 10 shows the solution to this problem using a context graph:

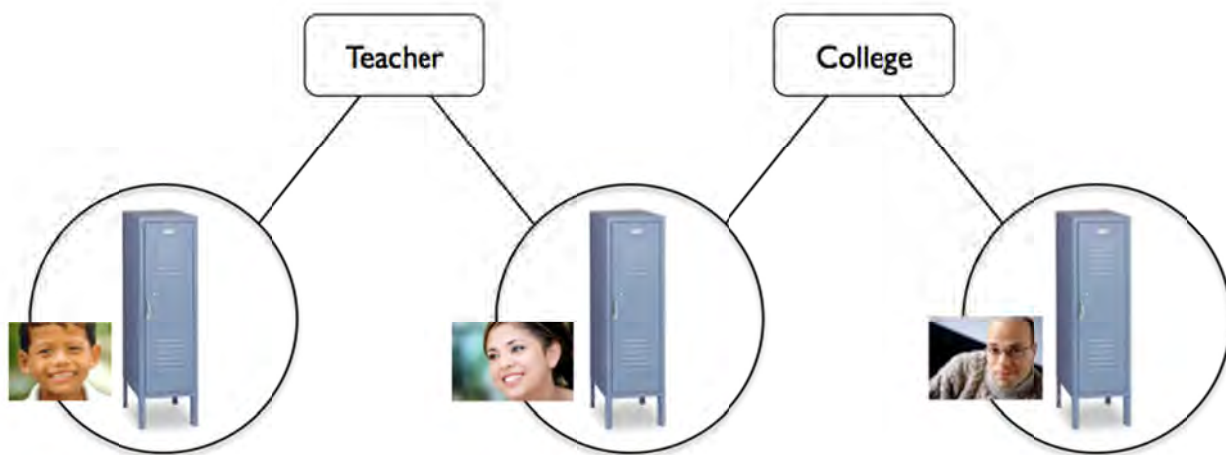


Figure 10: How contexts can solve the teacher/student friending problem

By connecting in context, a teacher can keep her student relationships separate from her college dormmate relationships. This makes it easy to share information appropriate to each context without fear that it will “leak out” into the wrong context.

On a personal network, the context graph is even more important (“context is king”) because the network itself is not intended to serve as a context. This is in contrast to many social networks where the network itself establishes a specific context, such as [Jumo](#) for non-profits, or the many specialized social networks on [Ning](#).²⁰

¹⁹ http://www.zephoria.org/thoughts/archives/2009/05/27/when_teachers_a.html

²⁰ <http://www.jumo.com/> and <http://www.ning.com/>

Vouching

Social networks support two basic types of relationships:

1. **Friending**, such as on Facebook (or “connecting” on LinkedIn), is a bi-directional or reciprocal link, i.e., one person must invite another and the invitee must accept the invitation to complete the link.
2. **Following**, such as on Twitter, is uni-directional or non-reciprocal link, i.e., one person can follow another without being followed back.

A personal network supports both these plus a third type of relationship called **vouching**. What is unique about vouching is:

- **It is a signal of trust and respect.** It is not just a sign that you know someone, but that you know they have a particular skill or expertise.
- **It is always in context.** Vouching is based on the context graph, so vouching relationships are always contextualized.
- **It is a gift.** The spirit of vouching is that of a [gift economy](#);²¹ as members of a personal network vouch for each other they make each other richer.

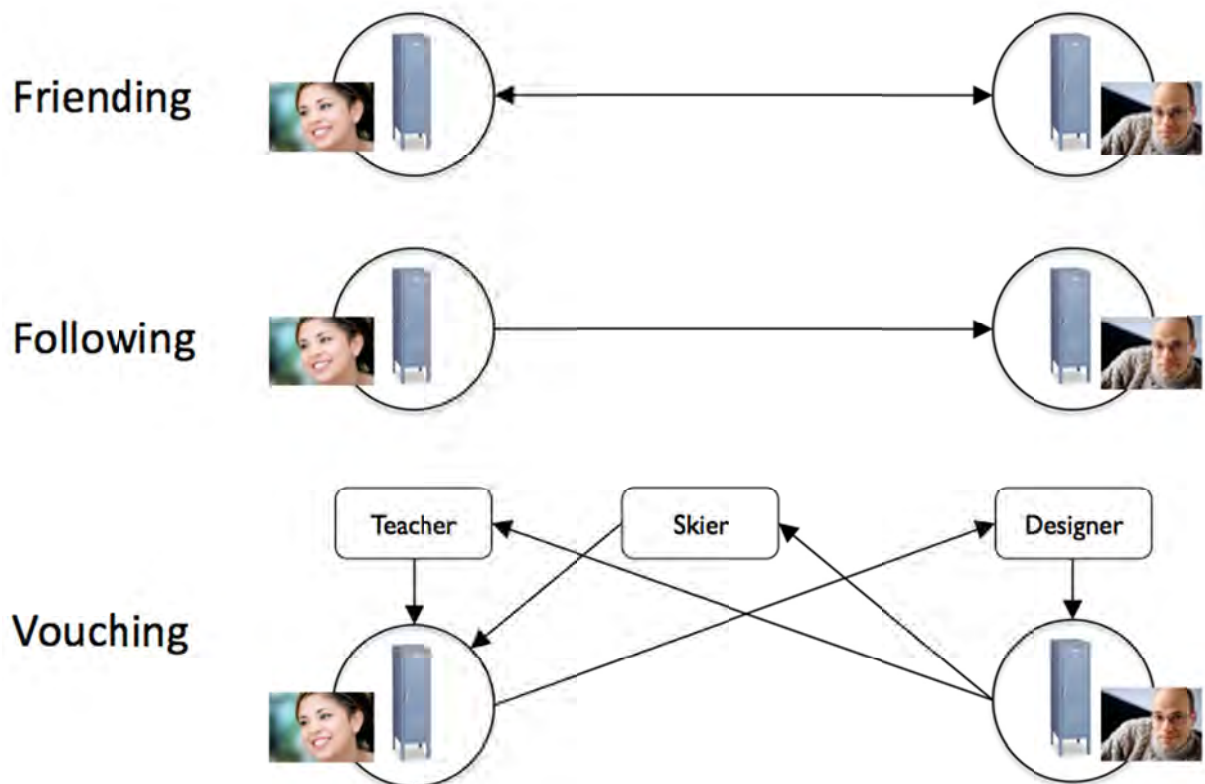


Figure 11: The differences between friending, following, and vouching

²¹ http://en.wikipedia.org/wiki/Gift_economy

Trust Anchors

Since every vouch is a signal of trust in a particular context, vouching relationships overlay a **trust graph** on top of the social graph. Trust graphs are the essence of what makes a personal network *personal*: they express not just who a person knows in what context, but who he/she personally trusts and respects in that context.

Trust graphs are what address the final principle in the Respect Trust Framework: **proof**. A trust graph provides social proof, through the relationships a person forms over time, of both his/her identity and his/her reputation in specific contexts.

This proof is highly valuable—both to the person and to his/her prospective contacts in any type of relationship, whether personal, social, professional, or commercial. In fact the combination of an individual's personal data with their social, context, and trust graphs—their **personal graph**—is so valuable that in January 2011 the World Economic Forum issued a new report titled [Personal Data: The Emergence of a New Asset Class](#).²² They summarize it by saying:

Personal data is becoming a new economic “asset class”, a valuable resource for the 21st century that will touch all aspects of society. This report finds that, to unlock the full potential of personal data, a balanced ecosystem with increased trust between individuals, government and the private sector is necessary.

According to [research by UK personal data analyst firm Ctrl-Shift](#), over the next ten years the market for **volunteered personal information**—data that individuals volunteer about who they are, what they want, what they are interested in, and what their goals and preferences are—will overtake the market for all other customer data in value, with access to VPI becoming the key strategic issue for companies dealing directly with customers.²³

Although this speaks to the business model for personal networks (see the next section), it is even more relevant to a greater social good: solving the problem of building a durable and sustainable trust fabric for the Internet. The urgency of this problem was highlighted by the announcement on 15 April 2011 of the U.S. [National Strategy for Trusted Identities in Cyberspace](#) (NSTIC).²⁴ In the introduction President Barack Obama states it this way:

The potential for fraud and the weakness of privacy protections often leave individuals, businesses, and government reluctant to conduct major transactions online. For example, providing patients with access to their medical records from their home computers requires that hospitals be able to confidently identify that patient online.

²² http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

²³ <http://ctrl-shift.co.uk/shop/product/51>

²⁴ <http://www.nist.gov/nstic/>

What the NSTIC calls the “identity ecosystem” needed to solve this problem has an even older name, the “[Web of trust](#)”.²⁵ This term originated not long after public/private key encryption technology was developed. Phil Zimmermann, creator of the [PGP \(Pretty Good Privacy\) encryption program](#),²⁶ envisioned a web of people who would sign each other’s PGP identity certificates. What was particularly original about Phil’s vision was that he saw this web of trust being rooted not in governments, banks, or other institutions, but in trust relationships between individuals. As he put it in the 1992 manual for PGP 2.0:

As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. ... This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.²⁷

Although PGP “key signing parties” were briefly popular in the early days of PGP, in-person key signing did not turn out to be practical in any significant scale. However, 20 years later, after the arrival of cloud computing and personal networks, all the necessary conditions are now present to realize this vision:

- The **social graphs** of relationships have been developed at the social layer.
- **Vouching** and **contexts** provide a way to layer on personal trust graphs.
- **Personal data lockers** and the **Respect Trust Framework** bring the degree of personal control necessary for trust graphs to be managed “in the cloud”.

All that remains is to define an explicit context for the “trusted introducer” relationship Phil envisioned. In the Respect Trust Framework this context is called a **trust anchor**. When one person vouches for another person as a trust anchor, it specifically means:

I trust this person to uphold the Respect Trust Framework.



Figure 12: One person vouching for another as a trust anchor

²⁵ http://en.wikipedia.org/wiki/Web_of_trust

²⁶ http://en.wikipedia.org/wiki/Pretty_Good_Privacy

²⁷ http://en.wikipedia.org/wiki/Web_of_trust, 2011-04-20

Founding Trust Anchors

As Phil Zimmermann's vision suggests, the role of a trust anchor is critical to establishing and maintaining trust on a personal network. After all, even though corporations or governments may join the network, a personal network is first and foremost a network of *people*, and trust must be rooted in these individuals.

Wikipedia is based on a similar premise. The [Reliability of Wikipedia](#) article states:

The Wikipedia model allows anyone to edit, and relies on a large number of well-intentioned editors to overcome issues raised by a smaller number of problematic editors. It is inherent in Wikipedia's editing model that misleading information can be added, but over time quality is anticipated to improve in a form of group learning as editors reach consensus, so that substandard edits will very rapidly be removed.²⁸

The Respect Trust Framework applies this same approach to building a trust network: the trust anchors essentially serve as the "Wikipedia admins" of reputation. It is not expected to be perfect, any more than Wikipedia is. But it is expected to be self-regulating and self-healing the same way Wikipedia is.

One key problem must still be addressed: how to bootstrap the chain of trust anchor vouching relationships so the network is not easily gamed. In reputation systems this type of vulnerability to the creation of multiple fake "sock puppet" accounts is called the [Sybil attack](#) after the famous case of multiple-personality disorder.²⁹

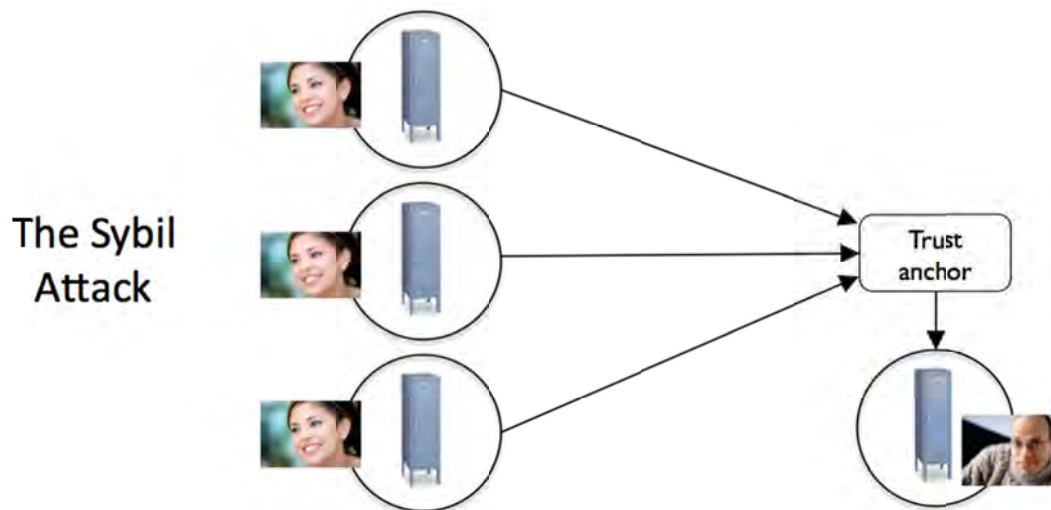


Figure 13: The Sybil attack: creating multiple accounts to game a reputation system

²⁸ http://en.wikipedia.org/wiki/Reliability_of_Wikipedia, 2011-04-20

²⁹ http://en.wikipedia.org/wiki/Sybil_attack

A 2005 paper by Alice Cheng and Eric Friedman called [Sybilproof Reputation Mechanisms](http://www.sigcomm.org/sigcomm2005/paper-CheFri.pdf)³⁰ proves mathematically that it is impossible to prevent Sybil attacks unless a reputation system establishes a known set of trusted users. So the solution defined in the Respect Trust Framework and being implemented by the Connect.Me Network is to enroll a set of **founding trust anchors**.

The enrollment process leverages personal trust relationships that already exist in the real world and the social networking world in two ways:

1. **In-person enrollment** will be held for members of the Internet identity, security, and privacy communities at four international conferences during the month of May 2011:
 - a. Internet Identity Workshop, May 3-5, Mountain View, USA
 - b. European Identity Conference, May 10-13, Munich, Germany
 - c. Telco 2.0/Personal Data 2.0, May 13, London, UK
 - d. Privacy/Identity/Innovation 2011, May 19-20, Santa Clara, USA
2. **A public nomination process** on the Twitter social messaging network will begin May 10. Any Twitter user may nominate another Twitter user simply by tweeting according to the instructions at **connect.me**.

Any other Twitter user may second the nomination by retweeting it. Nominees with sufficient support will be invited to become founding trust anchors (to prevent gaming, each nominee will be reviewed by previously enrolled trust anchors).

Once a critical mass of founding trust anchors is reached, further growth of the trust anchor community will proceed peer-to-peer via the Respect Trust Framework reputation rule shown in Figure 14: any individual member for whom **five existing trust anchors vouch as a trust anchor** becomes (at their option) a trust anchor.

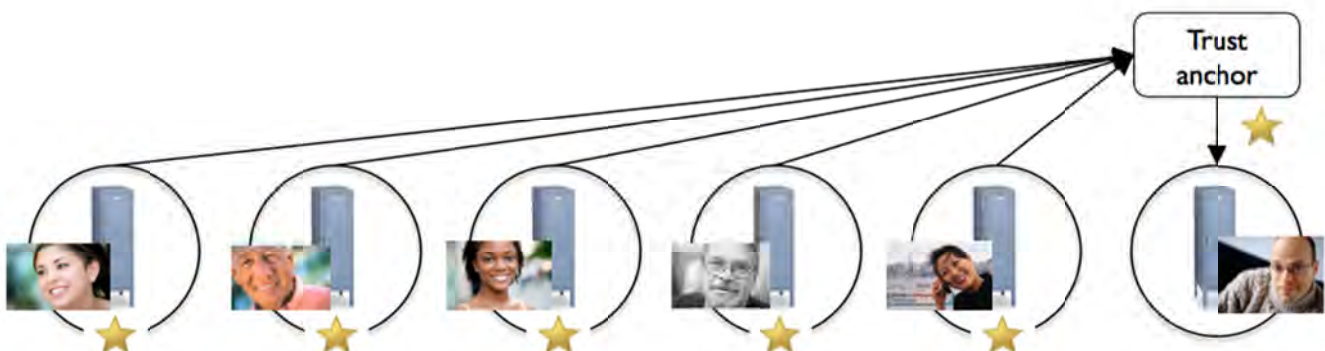


Figure 14: The five trust anchor vouching rule

³⁰ <http://www.sigcomm.org/sigcomm2005/paper-CheFri.pdf>

Part Four: The Business Model

To become a sustainable solution for safe sharing of personal data online—one that can be an integral component of the balanced ecosystem envisioned by the World Economic Forum and NSTIC—a personal network must have a sustainable business model. Most importantly, this model must enable personal network service providers to make money without exploiting the personal data of the members.

In fact, with proper legal and technical design, many service providers on a personal network can deliver their services **without even having access to that data**.

So how does a service provider acting in the trusted personal data agent role get paid?

One obvious analogy is to banking. Indeed, the previously cited World Economic Forum report about personal data as a new asset class goes so far as to say:

In practical terms, a person’s data would be equivalent to their “money.” It would reside in an account where it would be controlled, managed, exchanged and accounted for just like personal banking services operate today. These services would be interoperable so that the data could be exchanged with other institutions and individuals globally. ³¹

The banking analogy works well because banks have the same personal agent duty to protect their customer’s financial assets as personal network service providers have to protect their customer’s data assets.

But money and personal data are, as the WEF report highlights, **different asset classes**. For example, money can be lent: banks earn a profit by lending out customer deposits at a higher rate of interest than being paid to the customer.

Personal data cannot be “loaned out”: to do so would actually *diminish* its value. However, just as the value of money can only be realized by spending or loaning it, **the value of personal data can only be realized by sharing it**. Personal data that is never shared produces no more value than money stashed in a mattress.

It is the value of this sharing—*under personal control*—that provides the business model for personal networking just as the value of lending—*under bank control*—provides the business model for banking. This is summarized in Table 2:

Banks	Personal Network Providers
Earn money based on the market value of lending customer’s deposits	Earn money based on the market value of sharing customer’s personal data

Table 2: The business models of banking and personal networking

³¹ http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf, page 10

This form of commercially valuable data sharing relationship is shown in Figure 9 on page 12 as a **person-to-business connection**. From the standpoint of the business, this connection looks like an extension of their CRM system directly to the customer. Essentially, the business is “outsourcing” a portion of their relationship management directly to the customer by virtue of the personal network.³²

From a business perspective, this new form of outsourcing is **relationship-as-a-service**. The business is paying the personal network provider for a permissioned, bi-directional, highly trusted channel directly with a customer. The personal network provider in turn shares a portion of this revenue with the customer, just like a bank pays some of the interest it earns back to its customers.

This is a very different business model than advertising, the predominant economic fuel for social networks today. As writer Joel Stein observed in the March 10 Time Magazine cover story about [Your Data: For Sale](#):

You know how everything has seemed free for the past few years? It wasn't. It's just that no one told you that instead of using money, you were paying with your personal information.³³

To sustain their services, the third-party business model of social networks must leverage the personal data being shared with them to produce highly targeted advertising results. The personal data agent business model of personal networks effectively alters that option to require that the customer be provided with control.

Table 3 highlights the key differences between these two business models.

	Advertising (Social Network)	Relationship-as-a-Service (Personal Network)
Providers	Single provider	Multi-provider network
Data control	A third party (the social network) controls the data being shared with advertisers	The individual controls the data being shared with any party
Permission	Ads are not permissioned	All sharing is by permission
Relationship management	The third party mediates data sharing between the customer and the business	The customer and business manage their relationship directly
Customer benefit	Free services	Free services plus value earned from personal data

Table 3: The contrasting business models of advertising and relationship-as-a-service

³² From the standpoint of the customer, this is VRM – Vendor Relationship Management. See <http://blogs.law.harvard.edu/vrm/about/>

³³ <http://www.time.com/time/business/article/0,8599,2058114,00.html>

With its personal data agent business model, a personal network actually bears closer resemblance to a **credit card network** than to a social network. The strength of this analogy is illustrated in Table 4:

	Credit Card Network	Personal Network
Providers	Multi-provider network	Multi-provider network
Interoperability	Required	Required
Asset transacted	Money and credit	Personal data and reputation
Business model	Transaction fee	Relationship fee
Legal role	Agent to banks	Agent to individuals
API	Payment API	Personal API

Table 4: The analogy between credit card networks and personal networks

This analogy is particularly appropriate because the emergence of global credit card networks in the 1970s was a significant factor in building the market for consumer credit, as well as for the development of numerous ancillary services in the consumer finance ecosystem.

The same can be true now: the emergence of global personal networks has the potential to **build the market for personal data *not* in order to sell it, but to realize its full value in trusted relationships between people and businesses.** In fact, by moving the locus of control over personal data to individuals, and giving them choice, empowerment, and protection in the sharing of their personal data assets, personal networks can bring the advantages of social networks and credit card networks together into a rich new personal data ecosystem.

And, from an ethics perspective, only individuals are in a position to build this bridge because, as stated on the home page of the [Personal Data Ecosystem Consortium](http://personaldataecosystem.org/):

An individual user is the only ethical integration point for their own data from different sources.³⁴

³⁴ <http://personaldataecosystem.org/>, April 20 2011, based on a Jun 14 2007 blog post by Joe Andrieu, <http://blog.joeandrieu.com/2007/06/14/vrm-the-user-as-point-of-integration/>

Future Work

The principles of personal networks discussed in this white paper are not theoretical; the Respect Trust Framework will be announced at the European Identity Conference on May 10 2011, and the beta program for the first personal network operating under this trust framework, [Connect.Me](http://connect.me), will be launched at Privacy/Identity/Innovation 2011 on May 19.

But there is much more work to do to prove out the full potential of personal networks. Following are suggested forums and workstreams:

Open Identity Exchange (OIX)

OIX is a neutral non-profit home for open identity trust frameworks. The OIX Legal Analysis Working Group is already focused on legal issues related to trust frameworks, including contractual relationships, levels of assurance, levels of protection, and the "ecosystem of liabilities". The **OIX Respect Trust Framework Working Group** will focus on developing and iterating the ideas described in this white paper into further evolution of the Respect Trust Framework and related "plug-in" trust frameworks. Anyone may join an OIX Working Group—visit connect.me/trust for an invitation. <http://www.openidentityexchange.org/>

Personal Data Ecosystem Consortium (PDEC)

PDEC was founded to be the "voice of the individual" in the development of a personal data ecosystem. It also welcomes all the other stakeholders—businesses, policymakers, developers, investors—who want to contribute to the common infrastructure this ecosystem will require. PDEC will build community, gather and publish resources, coordinate open source projects, and provide end-user input and feedback to regulators. PDEC will also host the **Respect Trust Framework Discussion Forum**. <http://personaldataecosystem.org/>

World Economic Forum (WEF) Rethinking Personal Data Project

Launched in 2010, Rethinking Personal Data is a multi-year project intended to bring together private companies, public sector representatives, end-user privacy and rights groups, academics and topic experts to deepen the collective understanding of how a principled, collaborative and balanced personal data ecosystem can evolve. Contact jessica.lewis@weforum.org for more information. <http://www.weforum.org/issues/rethinking-personal-data/>

Mydex Community Interest Corporation (CIC)

Mydex CIC is a UK-based social enterprise based in the Young Foundation that is dedicated to helping people realize the value of their personal data online. Mydex CIC recently completed a working community prototype of a personal data ecosystem that successfully brought together large private and public-sector organizations into a user-driven and independently verified personal data service that gives total control to the user. Mydex is also developing a data model that scales to manage personal data of great complexity. For more information visit <http://mydex.org>.



This white paper is published by [Connect.Me](http://connect.me) under a [Creative Commons Attribution-ShareAlike 3.0 Unported License](http://creativecommons.org/licenses/by-sa/3.0/). For permissions beyond the scope of this license please contact info@connect.me. To download a current version, visit connect.me/trust.

Respect Trust Framework™, Respect Promise™, and Connect.Me™ are trademarks of Respect Network Corporation dba Connect.Me.